NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5

January 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA), 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. Such information security standards and guidelines shall not apply to national security systems without the express approval of the appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, OMB Director, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-53A Revision 5
Natl. Inst. Stand. Technol. Spec. Publ. 800-53A, Rev. 5, **733 pages** (January 2022)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5

Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts, practices, and methodologies may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review draft publications during the designated public comment periods and provide feedback to NIST. Many NIST publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Submit comments on this publication to: sec-cert@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

All comments are subject to release under the Freedom of Information Act (FOIA) [FOIA96].

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology (IT). ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information systems security and privacy and its collaborative activities with industry, government, and academic organizations.

Abstract

This publication provides a methodology and set of procedures for conducting assessments of security and privacy controls employed within systems and organizations within an effective risk management framework. The assessment procedures, executed at various phases of the system development life cycle, are consistent with the security and privacy controls in NIST Special Publication 800-53, Revision 5. The procedures are customizable and can be easily tailored to provide organizations with the needed flexibility to conduct security and privacy control assessments that support organizational risk management processes and are aligned with the stated risk tolerance of the organization. Information on building effective security and privacy assessment plans is also provided with guidance on analyzing assessment results.

Keywords

Assessment; assessment plan; assurance; control assessment; FISMA; Privacy Act; privacy controls; Open Security Controls Assessment Language; OSCAL; privacy requirements; Risk Management Framework; security controls; security requirements.

Acknowledgments

This publication was developed by the *Joint Task Force* Interagency Working Group. The group includes representatives from the civil, defense, and intelligence communities. The National Institute of Standards and Technology wishes to acknowledge and thank the senior leaders from the Department of Commerce, Department of Defense, the Office of the Director of National Intelligence, the Committee on National Security Systems, and the members of the interagency working group whose dedicated efforts contributed significantly to this publication.

Department of Defense

HON. John Sherman
Chief Information Officer

Dr. Kelly Fletcher
Principal Deputy Chief Information Officer

David McKeown
Deputy CIO for Cybersecurity and DoD CISO

Mark Hakun
Principal Deputy CIO for Cybersecurity

Kevin Dulany
Director, Cybersecurity Policy and Partnerships

Office of the Director of National Intelligence

Michael E. Waschull
Acting Chief Information Officer

Michael E. Waschull
Deputy Chief Information Officer

C. Matthew Conner
Cybersecurity Group and IC CISO

Cheri Benedict
Director, Security Coordination Center

National Institute of Standards and Technology

James St. Pierre
Acting Director, Information Technology Laboratory (ITL)

Kevin Stine
Cybersecurity Advisor, ITL

Matthew Scholl
Chief, Computer Security Division

Kevin Stine
Chief, Applied Cybersecurity Division

Victoria Yan Pillitteri
Risk Management Framework Project Leader

Committee on National Security Systems

Mark G. Hakun
Chair

Dominic A. Cussatt
Co-Chair

Kevin Dulany
Tri-Chair—Defense Community

Chris Johnson
Tri-Chair—Intelligence Community

Vicki Michetti
Tri-Chair—Civil Agencies

Joint Task Force (JTF) Working Group

Victoria Yan Pillitteri *NIST, JTF Leader*	Eduardo Takamura *NIST*	Kelley Dempsey *NIST*	Ron Ross *NIST*
McKay Tolboe *DoD*	Dave Myers *Veterans Affairs*	Vicki Michetti *Veterans Affairs*	Naomi Lefkovitz *NIST*
Andy Rovnak *Intelligence Community*	Peter Duspiva *Intelligence Community*	Chris Johnson *Intelligence Community*	Jessica Dickson *NIST*
Angela Smith *NIST*	Jon Boyens *NIST*	Ned Goren *NIST*	Kaitlin Boeckl *NIST*
Katie Isaacson *The MITRE Corporation*	Randy Gabel *The MITRE Corporation*	David Black *The MITRE Corporation*	Pam Miller *The MITRE Corporation*

In addition to the above acknowledgments, a special note of thanks goes to Jeff Brewer, Jim Foti, Cristina Ritfeld, Isabel Van Wyk, and the NIST web team for their outstanding administrative support, Chris Enloe for his technical review and insight, and to David Waltermire and Wendell Piez for their contribution to the development of the SP 800-53A assessment tables (both electronic sources, and derivative publications) using Open Security Controls Assessment Language (OSCAL). The authors also wish to recognize the professional staff from the NIST Computer Security Division and Applied Cybersecurity Division, and the representatives from the Federal Chief Information Officer (CIO) Council, Federal Chief Information Security Officer (CISO) Council, and Federal Privacy Council for their ongoing contributions in helping to improve the content of the publication. Finally, the authors gratefully acknowledge the contributions from individuals and organizations in the public and private sectors, both nationally and internationally, whose insightful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication.

HISTORICAL CONTRIBUTIONS TO NIST SPECIAL PUBLICATION 800-53A

The authors wanted to acknowledge the many individuals who contributed to previous versions of Special Publication 800-53A since its inception in 2005. They include Marshall Abrams, Dennis Bailey, Matt Barrett, Nadya Bartol, Frank Belz, Paul Bicknell, Deb Bodeau, Brett Burley, Bill Burr, Dawn Cappelli, Corinne Castanza, Matt Coose, George Dinolt, Donna Dodson, Randy Easter, Kurt Eleam, Jennifer Fabius, Daniel Faigin, Denise Farrar, Harriett Goldman, Peter Gouldmann, Richard Graubart, Jennifer Guild, Sarbari Gupta, Peggy Himes, Bennett Hodge, Cynthia Irvina, Arnold Johnson, Roger Johnson, Lisa Kaiser, Stu Katzke, Sharon Keller, Cass Kelly, Steve LaFountain, Steve Lipner, Bill MacGregor, Tom Macklin, Tom Madden, Erika McCallister, Tim McChesney, Michael McEvilley, John Mildner, Sandra Miravalle, Joji Montelibano, Doug Montgomery, George Moore, Harvey Newstrom, Robert Niemeyer, LouAnna Notargiacomo, Dorian Pappas, Tim Polk, Esten Porter, Karen Quigg, Steve Quinn, Ed Roback, George Rogers, Scott Rose, Mike Rubin, Karen Scarfone, Roger Schell, Matt Scholl, Murugiah Souppaya, Kevin Stine, Gary Stoneburner, Keith Stouffer, Marianne Swanson, Pat Toth, Glenda Turner, Joe Weiss, Richard Wilsher, Mark Wilson, John Woodward, and Carol Woody.

Document Conventions

For the purposes of this document, the term "security *and* privacy" is universally used since the guidance is applicable to both security and privacy control assessments. For certain systems, however, the guidance may only be relevant for ***security or privacy***. Organizations make their own determinations on when to manage security and privacy control assessments together or separately.

SP 800-53A provides guidance on assessing controls in information security program plans, privacy program plans, system security plans, and privacy plans. Where the guidance refers to all plans listed above, the term "security and privacy plans" is used. If the guidance is specific to a single type of plan (e.g., system security plan), the specific type of plan is specified.

Supplemental Content

The assessment procedures in Chapter 4 are published in multiple data formats, including comma-separated values (CSV), plain text, and Open Security Controls Assessment (OSCAL). The available data formats are accessible from the NIST SP 800-53A Revision 5, publication details page at https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final. The OSCAL Content Git Repository is available at https://github.com/usnistgov/oscal-content.

The CSV, plain text, and OSCAL formats represent derivative formats of the (normative) assessment procedures in this publication. If there are any discrepancies between the content in derivative formats and this publication, please contact sec-cert@nist.gov.

Patent Disclosure Notice

NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

DEVELOPING COMMON INFORMATION SECURITY AND PRIVACY FOUNDATIONS

COLLABORATION AMONG PUBLIC AND PRIVATE SECTOR ENTITIES

In developing standards and guidelines required by [FISMA], NIST consults with other federal agencies and offices as well as private sector entities to improve information security, avoid unnecessary and costly duplication of effort, and ensure that NIST publications complement the standards and guidelines employed for the protection of national security systems. In addition to its comprehensive public review and vetting process, NIST collaborates with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DoD), and the Committee on National Security Systems (CNSS) to establish and maintain a unified framework and common foundation for information security across the Federal Government. A common foundation and framework for information security provides the intelligence, defense, and civilian sectors of the Federal Government and their contractors more uniform and consistent ways to manage risks to organizational operations and assets, individuals, other organizations, and the Nation that result from the operation and use of systems. A common foundation and framework also provides a strong basis for the reciprocal acceptance of security authorization decisions and facilitate information sharing. NIST also works with public and private sector entities to establish and maintain specific mappings and relationships between the security standards and guidelines developed by NIST, the International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC).

ASSESSMENT PROCEDURE FORMATTING

The new format for assessment procedures introduced in Special Publication (SP) 800-53A Revision 4, is further improved in this revision (SP 800-53A Revision 5). The format continues to reflect the decomposition of assessment objectives into more *granular* determination statements wherever possible, thus providing the capability to identify and assess specific parts of security and privacy controls. Updates to SP 800-53A Revision 5:

- Identify determination statements for organization-defined parameters (ODPs) first and separately from the determination statements for each control item;
- Improve the readability of the assessment procedures;
- Provide a structured schema for automated tools when assessment information is imported into such tools;
- Provide greater flexibility in conducting assessments by giving organizations the capability to target certain aspects of controls (highlighting the particular weaknesses and/or deficiencies in controls),
- Improve the efficiency of security and privacy control assessments;
- Support continuous monitoring and ongoing authorization programs by providing a greater number of component parts of security and privacy controls that can be assessed at organization-defined frequencies and degrees of rigor.

The ability to apply assessment and monitoring resources in a targeted and precise manner and simultaneously maximize the use of automation technologies can result in more timely and cost-effective assessment processes for organizations.

Note: NIST [SP 800-53] will be updated accordingly to ensure that the numbering scheme for all security and privacy controls is consistent with the new format introduced in this publication.

Executive Summary

Security and privacy control assessments are not about checklists, simple pass/fail results, or generating paperwork to pass inspections or audits. Rather, control assessments are the principal vehicle used to verify that selected security and privacy controls are implemented and meeting stated goals and objectives. Special Publication (SP) 800-53A, *Assessing Security and Privacy Controls in Information Systems and Organizations*, facilitates security control assessments and privacy control assessments conducted within an effective risk management framework. A major design objective for SP 800-53A is to provide an assessment framework and initial starting point for assessment procedures that are flexible enough to meet the needs of different organizations while providing consistency in conducting control assessments. Control assessment results provide organizational officials with:

- Evidence of the effectiveness of implemented controls,
- An indication of the quality of the risk management processes, and
- Information about the security and privacy strengths and weaknesses of systems that are supporting organizational missions and business functions.

The findings identified by assessors are used to determine the overall effectiveness of security and privacy controls associated with systems and their environments of operation and to provide credible and meaningful inputs to the organization's risk management process. A well-executed assessment helps determine the validity of the controls contained in the organization's security and privacy plans and subsequently employed in organizational systems and environments of operation. Control assessments facilitate a cost-effective approach to managing risk by identifying weaknesses or deficiencies in systems, thus enabling the organization to determine appropriate risk responses in a disciplined manner that is consistent with organizational mission and business needs.

SP 800-53A is a companion guideline to [SP 800-53] *Security and Privacy Controls for Systems and Organizations*. Each publication provides guidance for implementing specific steps in the Risk Management Framework (RMF).[1] SP 800-53 and [SP 800-53B] address the Select step of the RMF and provide guidance on security and privacy control selection (i.e., determining the controls needed to manage risks to organizational operations and assets, individuals, other organizations, and the Nation). SP 800-53A addresses the Assess and Monitor steps of the RMF and provides guidance on the security and privacy control assessment processes. SP 800-53A also includes guidance on how to build effective assessment plans and how to analyze and manage assessment results.

SP 800-53A provides a process that allows organizations to tailor the assessment procedures outlined in the guidance. Tailoring involves customizing the assessment procedures to match the characteristics of the system and its environment of operation more closely. The tailoring process described in this guidance gives organizations the flexibility needed to avoid assessment approaches that are unnecessarily complex or costly while simultaneously meeting the assessment requirements and risk management principles established in the RMF. Tailoring decisions are left to the discretion of the organization to maximize flexibility in developing assessment plans – applying the results of risk assessments to determine the extent, rigor, and level of intensity of the assessments needed to provide sufficient assurance about the security and privacy posture of the system.

[1] [SP 800-37], *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* provides guidance on applying the RMF to systems and organizations.

Table of Contents

CHAPTER ONE

INTRODUCTION

THE NEED TO ASSESS SECURITY AND PRIVACY CONTROL EFFECTIVENESS

Today's systems[2] are complex assemblages of technology (i.e., hardware, software, and firmware), processes, and people working together to provide organizations with the capabilities to process, store, and transmit information in a timely manner in support of various mission and business functions. The degree to which organizations have come to depend upon systems to conduct routine, important, and critical mission and business functions means that the protection of the underlying systems and environments of operation is paramount to the success of the organization. The selection of appropriate security and privacy controls for a system is an important task that can have significant implications on the operations and assets of an organization as well as the welfare of individuals. Security controls are the safeguards or countermeasures prescribed for a system or an organization to protect the confidentiality, integrity, and availability of its system and information and to manage information security risk. Privacy controls are the administrative, technical, and physical safeguards employed within a system or an organization to manage privacy risks and ensure compliance with applicable privacy requirements.[3]

Once employed within a system, security and privacy controls are assessed to determine their overall effectiveness (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization). Understanding the overall effectiveness of implemented security and privacy controls is essential in determining the risk to the organization's operations and assets, individuals, other organizations, and the Nation resulting from the use of the system.

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide guidelines for building effective security and privacy assessment plans, as well as a comprehensive set of procedures for assessing the effectiveness of security and privacy controls employed in systems and organizations. The guidelines apply to the security and privacy controls defined in [SP 800-53] (as amended), *Security and Privacy Controls for Information Systems and Organizations*. The guidelines have been developed to help achieve more secure systems by:

- Enabling more consistent, efficient, comparable, and repeatable assessments of security and privacy controls with reproducible results;
- Promoting a better understanding of the risks to organizational operations, organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of systems;
- Facilitating more cost-effective assessments of security and privacy controls; and

[2] A system is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[3] OMB Circular A-130 [OMB A-130] defines security and privacy controls.

- Creating more complete, reliable, and trustworthy information for organizational officials to support risk management decisions, reciprocity of assessment results, information sharing, and compliance with federal laws, Executive Orders, directives, regulations, and policies.

This publication satisfies the requirements of Office of Management and Budget (OMB) Circular A-130 [OMB A-130] and the provisions of the Federal Information Security Modernization Act [FISMA]. The security and privacy guidelines in this publication are applicable to federal systems other than those systems designated as national security systems, as defined in 44 U.S.C., Section 3542. The guidelines have been broadly developed from a technical perspective to complement similar guidelines for national security systems and may be used for such systems with the approval of appropriate federal officials exercising policy authority over such systems. [4]

Organizations use this publication in conjunction with approved information security program plans, privacy program plans, system security plans, and privacy plans in developing assessment plans for producing and compiling the information necessary to determine the effectiveness of the security and privacy controls employed in the system and organization. The guidance in this publication has been developed with the intention of enabling organizations to tailor the basic assessment procedures provided. The assessment procedures are used as a starting point for and as input to the assessment plan. In developing effective security and privacy assessment plans, organizations take into consideration existing information about the controls to be assessed (e.g., results from assessments of risk; platform-specific dependencies in the hardware, software, or firmware; and any assessment procedures needed as a result of organization-specific controls not included in [SP 800-53]). [5]

The selection of appropriate assessment procedures and the rigor, intensity, and scope of the assessment depend on the following factors:

- The security categorization of the system; [6]
- The privacy risk assessment for the system;

[4] In accordance with the provisions of [FISMA] and OMB policy, whenever the interconnection of federal systems to systems operated by state/local/tribal governments, contractors, or grantees involves the processing, storage, or transmission of federal information, the information security standards and guidelines described in this publication apply. Specific information security requirements and the terms and conditions of the system interconnections are expressed in Memoranda of Understanding (MOU) and Interconnection Security Agreements (ISAs) established by participating organizations. For additional guidance on managing the security of information exchanges, see NIST [SP 800-47], Revision 1, *Managing the Security of Information Exchanges*.

[5] For example, detailed test scripts may need to be developed for the specific operating system, network component, middleware, or application employed within the system to adequately assess certain characteristics of a particular security or privacy control. Such test scripts are at a lower level of detail than provided by the assessment procedures contained in this guidance and are, therefore, beyond the scope of this publication.

[6] For national security systems, security categorization is accomplished in accordance with CNSS Instruction 1253 [CNSSI 1253]. For other than national security systems, security categorization is accomplished in accordance with Federal Information Processing Standard (FIPS) 199 [FIPS 199], NIST [SP 800-37], NIST [SP 800-60 Vol 1], NIST [SP 800-60 Vol 2], and the Controlled Unclassified Information (CUI) Registry [NARA CUI] as managed by the National Archives and Records Administration.

- The security and privacy controls from [SP 800-53] as identified in the approved information security program plans, privacy program plans, security plans, and privacy plans; [7] and
- The assurance requirements that the organization intends to meet in determining the overall effectiveness of the security and privacy controls.

The assessment process is an information-gathering activity of the as-implemented state of the system or common controls, not a security- or privacy-producing activity. Organizations determine the most cost-effective implementation of the assessment process by applying the results of risk assessments, considering the maturity and quality level of the organization's risk management processes, and taking advantage of the flexibility in the concepts described in this publication. The use of SP 800-53A as a starting point in the process of defining procedures for assessing the security and privacy controls in systems and organizations promotes the consistent application of security and privacy controls and offers the needed flexibility to customize the assessment based on organizational policies and requirements, known threat and vulnerability information, operational considerations, system and platform dependencies, and tolerance for risk. [8] The information produced during control assessments can be used by an organization to:

- Identify potential problems or shortfalls in the organization's implementation of the Risk Management Framework,
- Identify security- and privacy-related weaknesses and deficiencies in the system and in the environment in which the system operates,
- Prioritize risk response decisions and associated risk response activities,[9]
- Confirm that identified security- and privacy-related weaknesses and deficiencies in the system and in the environment of operation have been addressed,
- Support monitoring activities and information security and privacy situational awareness,
- Facilitate all types of system authorization decisions,[10] and
- Inform budgetary decisions and the capital investment process.

Organizations are not expected to employ all of the assessment methods and assessment objects contained within the assessment procedures identified in this publication for the associated security and privacy controls deployed within or available for inheritance by organizational systems. Rather, organizations have the inherent flexibility to determine the level of effort needed and the assurance required for a particular assessment (e.g., which assessment methods and assessment objects are most useful in obtaining the desired results). Determination of the level of effort and required assurance is made based on what is

[7] The security and privacy controls for the system and organization are documented in the system security plans and privacy plans after the initial selection and tailoring of the controls, as described in [SP 800-53] and [CNSSI 1253]. The Program Management controls are documented in information security program plans and privacy program plans, as described in SP 800-53.

[8] In this publication, the term risk is used to mean risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.

[9] [SP 800-39] provides additional information about the types of risk response.

[10] Types of authorization decisions are described in [SP 800-37], Appendix F.

necessary to accomplish the assessment objectives in the most cost-effective manner and with sufficient confidence to support the subsequent determination of the resulting mission or business risk (i.e., risk management). Organizations balance the resources expended on the deployment of security and privacy controls (i.e., safeguards and countermeasures implemented for security and privacy protection) with the resources expended to determine overall control effectiveness, both initially and on an ongoing basis through continuous monitoring programs.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse group of system and information security and privacy professionals, including:

- Individuals with system development responsibilities (e.g., program managers, system designers and developers, systems integrators, information security engineers and privacy engineers);
- Individuals with information security and privacy assessment and monitoring responsibilities (e.g., Inspectors General, system evaluators, assessors, independent verifiers/validators, auditors, analysts, system owners, common control providers);
- Individuals with system, security, privacy, risk management, and oversight responsibilities (e.g., authorizing officials, chief information officers, senior information security officers,[11] senior agency officials for privacy/chief privacy officers, system managers, information security and privacy managers); and
- Individuals with information security and privacy implementation and operational responsibilities (e.g., system owners, common control providers, information owners/stewards, mission and business owners, system administrators, system security officers, system privacy officers).

1.3 RELATED PUBLICATIONS AND ASSESSMENT PROCESSES

SP 800-53A is designed to support [SP 800-37], *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. In particular, the assessment procedures contained in this publication and the guidelines provided for developing security and privacy assessment plans for organizational systems directly support the assessment and monitoring activities that are integral to the risk management process. The integral activities include providing near real-time security- and privacy-related information to organizational officials regarding the ongoing security and privacy state of their systems and organizations.

Organizations are encouraged to take advantage of the control assessment results and associated assessment documentation, artifacts, and evidence available for system components from previous assessments, including independent third-party testing, evaluation, and validation.[12] Product testing, evaluation, and validation may be conducted on

[11] At the federal *agency* level, the role is known as the Senior Agency Information Security Officer. Organizations may also refer to the role as the *Senior Information Security Officer* or the *Chief Information Security Officer*.

[12] Assessment results can be obtained from many activities that occur routinely during the system development life cycle. For example, assessment results are produced during the testing and evaluation of new system components

cryptographic modules and general-purpose information technology products, such as operating systems, database systems, firewalls, intrusion detection systems, web browsers, web applications, smart cards, biometrics devices, personal identity verification devices, network devices, and hardware platforms using national and international standards. If a system component product is identified as providing support for the implementation of a particular control in [SP 800-53], then evidence produced during the product testing, evaluation, and validation processes (e.g., security or privacy specifications, analyses and test results, validation reports, and validation certificates)[13] is used to the extent that it is applicable. The applicable product testing evidence can be combined with the assessment-related evidence obtained from the application of the assessment procedures in this publication to cost-effectively produce the information necessary to determine whether the security and privacy controls are effective in their application.

1.4 ORGANIZATION OF THIS PUBLICATION

The remainder of this publication is organized as follows:

- **Chapter Two** describes the fundamental concepts associated with security and privacy control assessments, including the integration of assessments into the system development life cycle, the importance of an organization-wide strategy for conducting security and privacy control assessments, the development of effective assurance cases to help increase grounds for confidence in the effectiveness of the security and privacy controls being assessed, and the format and content of assessment procedures.
- **Chapter Three** describes the process of assessing the security and privacy controls in organizational systems and their environments of operation, including the activities carried out by organizations and assessors to prepare for security and privacy control assessments; the development of security assessment plans; the conduct of security and privacy control assessments; the analysis, documentation, and reporting of assessment results; and the post-assessment report analysis and follow-on activities carried out by organizations.
- **Chapter Four** provides a catalog of security and privacy assessment procedures that can be used to develop plans for assessing security controls.
- **Supporting appendices** provide detailed assessment-related information, including general references, definitions and terms, acronyms, a description of assessment methods, penetration testing guidelines, content of security and privacy assessment reports, and automation support for ongoing assessments.

during system upgrades or system integration activities. Organizations can take advantage of previous assessment results whenever possible, to reduce the overall cost of assessments and to make the assessment process more efficient.

[13] Organizations review the available information from component information technology products to determine what security and privacy controls are implemented by the product, if those controls meet the intended control requirements of the system under assessment, if the configuration of the product and the environment in which the product operates are consistent with the environmental and product configuration stated by the vendor and/or developer, and if the assurance requirements stated in the developer/vendor specification satisfy the assurance requirements for assessing those controls. Meeting the above criteria provides a sound rationale that the product is suitable and meets the intended security and privacy control requirements of the system under assessment.

CHAPTER TWO

THE FUNDAMENTALS

BASIC CONCEPTS ASSOCIATED WITH SECURITY AND PRIVACY CONTROL ASSESSMENTS

This chapter describes the basic concepts associated with assessing the security and privacy controls in organizational systems and the environments in which those systems operate, including the integration of assessments into the system development life cycle, the importance of an organization-wide strategy for conducting assessments, the development of effective assurance cases to help increase grounds for confidence in the effectiveness of security and privacy controls, and the format and content of assessment procedures. A fundamental design objective for SP 800-53A is to provide a flexible assessment framework and a starting point for assessment procedures to be used by different organizations and systems while providing a repeatable approach to facilitate consistency in conducting control assessments.

2.1 ASSESSMENTS WITHIN THE SYSTEM DEVELOPMENT LIFE CYCLE

Security and privacy assessments can be carried out throughout system development life cycle phases[14] to increase grounds for confidence that the security and privacy controls employed within or inherited by a system are effective in their application. The guidance in this publication provides a comprehensive set of assessment procedures to support security and privacy assessment activities throughout the system development life cycle. For example, security and privacy assessments are routinely conducted during the development/acquisition and implementation phases of the life cycle. Conducting assessments during the development/acquisition and implementation phases helps ensure that the required controls for the system are designed and developed consistent with risk management goals, correctly implemented, and consistent with the established organizational information security and privacy architecture before the system enters the operations and maintenance phase. Security and privacy assessments conducted in pre-operational system development life cycle phases include design and code reviews, application scanning, regression testing, and ensuring that applicable privacy laws and policies are adhered to and that privacy protections are embedded in the design of the system.

Security- and privacy-related weaknesses and deficiencies identified early in the system development life cycle can be resolved more quickly and cost-effectively than deficiencies identified in subsequent phases of the life cycle. Early identification of security- and privacy-related weaknesses and deficiencies in the selected security and privacy controls facilitates determination and implementation of appropriate risk responses and allows for effectiveness of control implementations to be validated during system design and testing.

Security and privacy assessments are also conducted during the operations and maintenance phase of the life cycle to ensure that the controls continue to be effective in the operational environment and protect against constantly evolving risks. Organizations assess all security and privacy controls employed within and inherited by the system during the initial system

[14] There are typically five phases in a generic system development life cycle: (i) initiation, (ii) development/acquisition, (iii) implementation, (iv) operations and maintenance, and (v) disposition (disposal).

authorization. Following the initial authorization, the organization assesses all implemented security and privacy controls on an ongoing basis in accordance with its Information Security Continuous Monitoring (ISCM) strategy and privacy continuous monitoring strategy.[15] The ongoing assessment and monitoring of controls use the assessment procedures defined in this publication. The frequency of such assessments and monitoring is determined by the organization, system owner, and/or common control provider and is approved by the authorizing official. Finally, at the end of the life cycle, security and privacy assessments are conducted to ensure that important organizational information, including personally identifiable information, are purged from the system prior to disposal and organizational retention schedules are adhered to.

2.2 CONTROL STRUCTURE AND ORGANIZATION

Organizations are encouraged to develop a broad-based, organization-wide strategy for conducting security and privacy assessments to facilitate more cost-effective and consistent assessments across the inventory of systems. Maximizing the number of common controls employed within an organization significantly reduces the costs of development, implementation, and assessment of security and privacy controls; allows organizations to centralize and automate control assessments and amortize the cost of those assessments across all systems in the organization; and increases the consistency of security and privacy control implementations.

THE BENEFIT OF IMPLEMENTATION AND ASSESSMENT OF COMMON CONTROLS AND SHARING ASSESSMENT RESULTS

An organization-wide approach to identifying common controls early in the application of the RMF facilitates a more global strategy for assessing those common controls and sharing assessment results with system owners and authorizing officials. The sharing of assessment results among key organizational officials across system boundaries has many important benefits, including:

- Providing the capability to review assessment results for all systems and to make mission and business-related decisions on risk mitigation activities according to organizational priorities, the security categorization of the systems, and risk assessment results;
- Providing a more global view of systemic weaknesses and deficiencies occurring in systems across the organization and an opportunity to develop organization-wide solutions to information security and privacy problems; and
- Increasing the organization's knowledge base regarding threats, vulnerabilities, privacy risks, and strategies for more cost-effective solutions to common information security and privacy problems.

Organizations can also promote a more focused and cost-effective assessment process by developing specific assessment procedures that are tailored to their specific environments of operation and requirements (instead of relegating assessment procedure development tasks to individual control assessors or assessment teams) and by providing organization-wide tools,

[15] [SP 800-137] provides guidance on the continuous monitoring of security controls as part of an ISCM Program. Continuous monitoring can be applied effectively to privacy controls consistent with the concepts, techniques, and principles described in SP 800-137. Senior Agency Officials for Privacy (SAOPs)/Chief Privacy Officers (CPOs) provide guidance on the ongoing monitoring of privacy controls. NIST Interagency Report 8011 [NISTIR 8011], *Automation Support for Security Control Assessments*, provides guidance on methods to automate the assessment process.

templates, and techniques to support more consistent assessments throughout the organization. [16]

The roles responsible for conducting control assessments may include system owners, common control providers, system security and privacy officers, independent assessors, auditors, and Inspectors General with oversight by the authorizing official(s).[17] There is also significant involvement in the assessment process of other parties within the organization who have a vested interest in the outcome of assessments. Other interested parties include mission and business owners and information owners/stewards (when those roles are filled by someone other than the system owner). It is imperative that system owners and common control providers identify and coordinate with other parties in the organization that have an interest in control assessments to help ensure that the organization's core missions and business functions are adequately addressed in the assessment of security and privacy controls.

CAUTIONARY NOTE

Organizations carefully consider the potential impacts of employing the assessment procedures defined in this publication when assessing the security and privacy controls in *operational* systems. Certain assessment procedures – particularly those that directly impact the operation or function of the hardware, software, or firmware components of a system – may inadvertently affect the routine processing, transmission, or storage of information that supports organizational missions or business functions. For example, a critical system component may be taken offline for assessment purposes, or a component may suffer a fault or failure during the assessment process. Organizations take the necessary precautions to ensure that organizational missions and business functions continue to be supported by systems and that any potential impacts to operational effectiveness resulting from assessment activities are considered in advance.

2.3 BUILDING AN EFFECTIVE ASSURANCE CASE

Building an effective assurance case[18] for security and privacy control effectiveness is a process that involves compiling evidence from a variety of activities conducted during the system development life cycle that the controls employed in the system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements of the system and the organization and presenting the evidence in a manner that decision makers are able to use effectively in making risk-based decisions about the operation or use of the system (i.e., to manage risk). The evidence described above comes from

[16] Organizations may also provide security and privacy control assessment plans, including tailored assessment procedures, to external service providers who are operating systems on behalf of those organizations. In addition, tailored control and privacy assessment plans can recommend supporting templates, tools, and techniques and also be further tailored to the contract with the service provider, helping to make assessments more consistent and to maximize the reuse of assessment-related artifacts. The reuse of artifacts can improve security and privacy through uniformity and reduce/eliminate contracting ambiguity, resulting in reduced costs and risk to the organization.

[17] In accordance with [OMB A-130], an independent evaluation of privacy program and practices is not required. However, an organization may choose to employ independent privacy assessments at the organization's discretion.

[18] An assurance case is a body of evidence organized into an argument demonstrating that some claim about a system holds (i.e., is assured). An assurance case is needed when it is important to show that a system exhibits some complex property, such as safety, security, privacy, or reliability.

the implementation of the security and privacy controls in the system and inherited by the system (i.e., common controls) and from the assessments of that implementation. Ideally, the assessor builds on previously developed materials that started with the specification of the organization's information security and privacy needs and was further developed during the design, development, and implementation of the system. The materials developed while implementing security and privacy throughout the life cycle of the system provide the initial evidence for an assurance case.

During the assessment process, assessors obtain the evidence needed to allow the appropriate organizational officials to make objective determinations about the effectiveness of the security and privacy controls and the overall security and privacy state of the system. The assessment evidence needed to make such determinations can be obtained from a variety of sources, including information technology product and system assessments and – in the case of privacy assessments – documentation such as privacy impact assessments and Privacy Act system of record notices. Product assessments (also known as product testing, evaluation, and validation) are typically conducted by independent, third-party testing organizations. Assessments examine the security and privacy functions of products and established configuration settings. Assessments can be conducted to demonstrate compliance with industry, national, or international information security and privacy standards and developer/vendor claims. Since many information technology products are assessed by commercial testing organizations and then subsequently deployed in millions of systems, product assessments can be carried out at a greater level of depth and provide deeper insights into the security and privacy capabilities of the particular products.

System and common control assessments are typically conducted by system developers, system integrators, system owners, common control providers, assessors, auditors, Inspectors General, and organizational information security and privacy personnel. The assessors or assessment teams bring together available information about the system or common control, such as the results from individual component product assessments, information in the system security and privacy plans, other system/common control documentation, or previous assessment results, and conduct additional system-level or common control assessments using a variety of methods and techniques. System and common control assessments are used to compile and evaluate the evidence needed by organizational officials to determine how effectively the security and privacy controls employed in systems mitigate risks to organizational operations and assets, individuals, other organizations, and the Nation. The results of assessments conducted using system-specific and organization-specific assessment procedures derived from the guidelines in this publication contribute to compiling the necessary evidence to determine security and privacy control effectiveness in accordance with the assurance requirements documented in security and privacy plans.

Assurance Evidence from Developmental and Operational Activities

Organizations obtain security and privacy assurance by the actions taken by system developers, implementers, operators, maintainers, and assessors. Actions by individuals and/or groups during the development/operation of systems produce security and privacy evidence that contributes to the assurance, or measures of confidence, in the security and privacy functionality needed to deliver the security and privacy capability. The depth and coverage of these actions (as described in Appendix C) also contribute to the efficacy of the evidence and

measures of confidence. The evidence produced by developers, implementers, operators, assessors, and maintainers during the system development life cycle (e.g., design/development artifacts and assessment results) contributes to the understanding of the effectiveness of security and privacy controls implemented by organizations.

The strength of the security and privacy functionality[19] plays an important part in achieving the desired capabilities and subsequently satisfying the security and privacy requirements of organizations. System developers can increase the strength of security and privacy functionality by employing well-defined security and privacy policies and procedures, structured and rigorous design and development techniques, and sound system, security, and privacy engineering techniques as part of the system development process. The artifacts generated by development activities (e.g., functional specifications, system design documentation, and the results of testing and code analysis) can provide important evidence that systems and their components are more reliable and trustworthy. Security and privacy evidence can also be generated from testing conducted by independent, third-party assessment organizations and other assessment activities conducted by government and private sector organizations.[20]

In addition to the evidence produced in the development environment, organizations can produce evidence from the operational environment that contributes to the assurance of functionality and security and privacy capabilities. Operational evidence includes records of remediation actions, the results of security incident reporting (including breaches involving personally identifiable information), and the results of organizational continuous monitoring activities. Such evidence helps determine the effectiveness of deployed security and privacy controls, changes to systems and environments of operation, and compliance with legislation, policies, directives, regulations, and standards. Security and privacy evidence – whether obtained from development or operational activities – helps organizations determine the extent to which their systems are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting stated security and privacy requirements, thus providing greater assurance in the system's security and privacy capabilities.

The depth and coverage of security and privacy evidence can affect the level of assurance in the functionality implemented. Depth and coverage are attributes associated with assessment methods and the generation of security and privacy evidence.[21] Assessment methods can be applied to support developmental and operational assurance. For developmental assurance, depth is associated with the rigor, level of detail, and formality of the artifacts produced during system design and development. The level of detail available in development artifacts can affect the type of testing, evaluation, and analysis conducted during the system development life cycle (e.g., basic testing, comprehensive testing, and focused testing, static/dynamic analysis). For operational assurance, the depth attribute addresses the rigor and level of detail for the

[19] The security or privacy *strength* of a system component (i.e., hardware, software, or firmware) is determined by the degree to which the security or privacy functionality implemented within that component is correct, complete, resistant to direct attacks (strength of mechanism), and resistant to bypass or tampering.

[20] For example, third-party assessment organizations assess cloud services and service providers in support of the Federal Risk and Authorization Management Program [FedRAMP]. Common Criteria Testing Laboratories test and evaluate information technology products using [ISO 15408]. Cryptographic/Security Testing Laboratories test cryptographic modules using the [FIPS 140-3] standard.

[21] For additional information about depth and coverage, see Section 2.4 and Appendix C.

assessment. In contrast, the coverage attribute is associated with the assessment methods employed during development and operations, addressing the scope and breadth of assessment objects included in the assessments (e.g., number and types of tests conducted on source code).

2.4 ASSESSMENT PROCEDURES: ASSESSMENT OBJECTS, METHODS AND OBJECTIVES

An assessment ***procedure*** consists of a set of assessment *objectives*, each with an associated set of potential assessment *methods* and assessment *objects*. An assessment objective includes one or more *determination statements* related to the [SP 800-53] control under review. The determination statements are linked to the content of the control (i.e., the security and privacy control functionality) to ensure the traceability of assessment results back to the fundamental control requirements. The application of an assessment procedure to a control produces assessment findings.[22] Assessment findings reflect or are subsequently used to help determine the overall effectiveness of the control and help the authorizing official make an informed, risk-based decision on whether to place the system into operation or continue its operation.

2.4.1 ASSESSMENT OBJECTS

Assessment ***objects*** identify the specific items being assessed as part of a given control and include *specifications*, *mechanisms*, *activities*, and *individuals*. Specifications are the document-based artifacts (e.g., policies, procedures, plans, system security and privacy requirements, functional specifications, architectural designs) associated with a system or common control. Mechanisms are the specific hardware, software, or firmware safeguards and countermeasures employed within a system or common control.[23] Activities are the specific protection-related actions supporting a system or common control that involve people (e.g., conducting system backup operations, monitoring network traffic, exercising a contingency plan). Individuals or groups of individuals are people applying the specifications, mechanisms, or activities described above.

2.4.2 ASSESSMENT METHODS

Assessment ***methods*** define the nature of the assessor actions and include examine, interview, and test.

- The *examine* method is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities) to facilitate assessor understanding, achieve clarification, or obtain evidence.
- The *interview* method is the process of holding discussions with individuals or groups of individuals within an organization to facilitate assessor understanding, achieve clarification, or obtain evidence.
- The *test* method is the process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare the actual state of the object to the desired state or expected behavior of the object.

[22] For more information about control assessment findings, see Section 3.3.

[23] Mechanisms also include physical protection devices associated with a system or common control (e.g., locks, keypads, security cameras, fire protection devices, fireproof safes, etc.).

In all three assessment methods, the results are used to make specific determinations called for in the determination statements and thereby achieve the objectives for the assessment procedure. A complete description of assessment methods and assessment objects is provided in Appendix C.

Assessment methods have a set of associated attributes – *depth* and *coverage* – which help define the level of effort for the assessment. The attributes are hierarchical in nature, providing the means to define the rigor and scope of the assessment for the increased assurances that may be needed for some systems.

- The depth attribute addresses the rigor and level of detail in the examination, interview, and testing processes. Values for the depth attribute include *basic*, *focused*, and *comprehensive*.
- The coverage attribute addresses the scope or breadth of the examination, interview, and testing processes, including the number and types of specifications, mechanisms, and activities to be examined or tested and individuals to be interviewed. Similar to the depth attribute, values for the coverage attribute include *basic*, *focused*, and *comprehensive*.

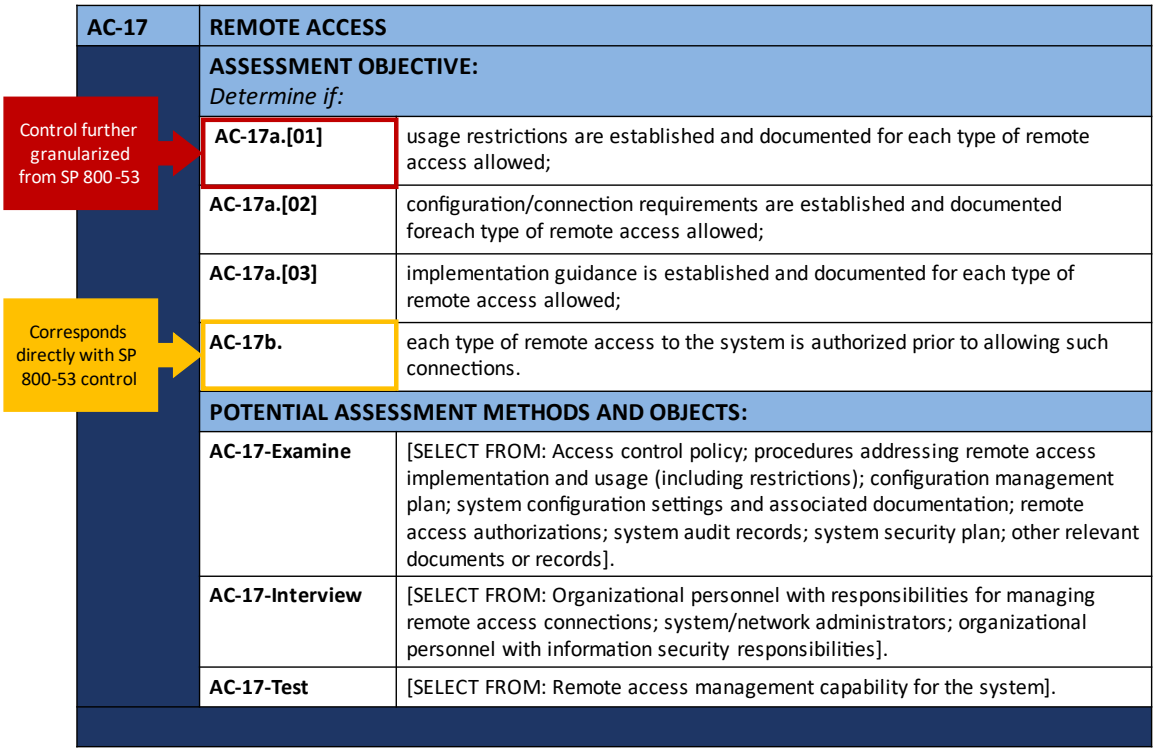
The appropriate depth and coverage attribute values for a particular assessment method are based on the assurance requirements specified by the organization and are an important component of protecting information commensurate with risk (i.e., risk management). As assurance requirements increase with regard to the development, implementation, and operation of controls within or inherited by the system, the rigor and scope of the assessment activities (as reflected in the selection of assessment methods and objects and the assignment of depth and coverage attribute values) tend to increase as well.[24] Appendix C provides a detailed description of assessment method attributes and attribute values.

2.4.3 ASSESSMENT OBJECTIVES

The assessment objectives are numbered sequentially, first in accordance with the numbering scheme in [SP 800-53] and, subsequently, where necessary to further granularize the security or privacy control requirements to facilitate assessment. Square bracketed sequential numbers, as opposed to parentheses, are used to indicate that the control from SP 800-53 has been further granularized (e.g., AC-17a.[01], AC-17a.[02], AC-17a.[03]).

[24] The level of effort for the assessment, including the depth and coverage, is primarily determined by the privacy risk assessment or security categorization of the system or common control being assessed.

Figure 1 illustrates an example assessment procedure developed to assess the effectiveness of control AC-17. The assessment objective for AC-17 is derived from the base control statement described in [SP 800-53]. AC-17a.[01] is an example of a determination statement for a control item that is further granularized from SP 800-53. AC-17b. is an example of a determination statement for a control item that corresponds directly with the SP 800-53 control. Potential assessment methods and objects are added to each assessment procedure. Not all assessment procedures include all three potential assessment methods (i.e., examine, interview, test). The organization determines the assessment methods needed to provide the level of assurance required by the organization.



AC-17	REMOTE ACCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-17a.[01]	usage restrictions are established and documented for each type of remote access allowed;
	AC-17a.[02]	configuration/connection requirements are established and documented foreach type of remote access allowed;
	AC-17a.[03]	implementation guidance is established and documented for each type of remote access allowed;
	AC-17b.	each type of remote access to the system is authorized prior to allowing such connections.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-17-Examine	[SELECT FROM: Access control policy; procedures addressing remote access implementation and usage (including restrictions); configuration management plan; system configuration settings and associated documentation; remote access authorizations; system audit records; system security plan; other relevant documents or records].
	AC-17-Interview	[SELECT FROM: Organizational personnel with responsibilities for managing remote access connections; system/network administrators; organizational personnel with information security responsibilities].
	AC-17-Test	[SELECT FROM: Remote access management capability for the system].

FIGURE 1: ASSESSMENT PROCEDURE FOR A CONTROL

Another example of granularization to support control assessments is the case of a privacy control requirement not being applicable to a particular system (e.g., the system does not process personally identifiable information); assessors can disregard such non-applicable requirements and still find that the control is satisfied. Figure 2 provides an example of control CM-04[25], which is further granularized to address security impacts in CM-04[01] and privacy impacts in CM-04[02].

CM-04	IMPACT ANALYSES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-04[01]	changes to the system are analyzed to determine potential security impacts prior to change implementation;
	CM-04[02]	changes to the system are analyzed to determine potential privacy impacts prior to change implementation.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-04-Examine	[SELECT FROM: Configurat cedures addressing security impact analyses f ocedures addressing privacy impact analyses fo figuration management plan; security impact anal mpact analysis documentation; privacy impact assessment; privacy risk assessment documentation, system design documentation; analysis tools and associated outputs; change control records; system audit records; system security plan; privacy plan; other relevant documents or records].
	CM-04-Interview	[SELECT FROM: Organizational personnel with responsibility for conducting security impact analyses; organizational personnel with responsibility for conducting privacy impact analyses; organizational personnel with information security and privacy responsibilities; system developer; system/network administrators; members of change control board or similar].
	CM-04-Test	[SELECT FROM: Organizational processes for security impact analyses; organizational processes for privacy impact analyses].

Granularized to address privacy impacts separate from security impacts

FIGURE 2. ASSESSMENT PROCEDURE FOR A CONTROL FURTHER GRANULARIZED TO FACILITATE ASSESSMENT

Additionally, determination statements for organization-defined parameters (ODPs) are listed first and separately from the determination statements for each control item within each control or control enhancement to enable the assessor to quickly determine whether the ODPs are defined or selected by the organization. ODPs appear first in the determination statements, and each include a unique identifier associated with the control to facilitate a more efficient and streamlined assessment. ODPs include:

- **Assignment operations**, where the organization defines a value (e.g., frequency, circumstances, personnel, or roles)
- **Selection operations**, where the organization selects one or more of the options provided in the ODP

The ODP numbering convention is "**XX-nn_ODP"**, where XX is the two-character control family abbreviation, and nn is the control number (with a leading zero for single digits) followed by

[25] Note that the control identifiers (e.g., CM-4), as published in [SP 800-53], do not include a leading zero. Future revisions of SP 800-53 control identifiers will include a leading zero (e.g., CM-04).

"_ODP". If there is more than one ODP for the assessment procedure, "_ODP" is followed by square-bracketed sequential numbers starting from "01". The ODP value is referenced in subsequent determination statements using the ODP unique identifier and a short phrase describing the ODP surrounded by < >. Similar to declaring a variable in computer programming, the ODP serves as a symbolic name to reference a stored value. In this scenario, the ODP unique identifier serves as the symbolic name, and the value assigned or selected by the organization is the stored value.

Figure 3 provides an example of an assessment procedure for control CM-02 that includes two assignment operations: CM-02_ODP[01] and CM-02_ODP[02].

CM-02	BASELINE CONFIGURATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-02_ODP[01]	***the frequency of baseline configuration review and update is defined;***
	CM-02_ODP[02]	***the circumstances requiring baseline configuration review and update are defined;***
	CM-02a.[01]	a current baseline configuration of the system is developed and documented;
	CM-02a.[02]	a current baseline configuration of the system is maintained under configuration control;
	CM-02b.01	the baseline configuration of the system is reviewed and updated ***<CM-02_ODP[01] frequency>***;
	CM-02b.02	the baseline configuration of the system is reviewed when required due to ***<CM-02_ODP[02] circumstances>;***
	CM-02b.03	the baseline configuration of the system is reviewed when system components are installed or upgraded.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-02-Examine	[SELECT FROM: Configuration management policy; procedures addressing the baseline configuration of the system; configuration management plan; enterprise architecture documentation; system design documentation; system security plan; privacy plan; system architecture and configuration documentation; system configuration settings and associated documentation; system component inventory; change control records; other relevant documents or records].
	CM-02-Interview	[SELECT FROM: Organizational personnel with configuration management responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	CM-02-Test	[SELECT FROM: Organizational processes for managing baseline configurations; automated mechanisms supporting configuration control of the baseline configuration].

Organization-Defined Parameter (ODP) identifier

Assignment Statement

Reference to ODP in determination statement

FIGURE 3. ASSESSMENT PROCEDURE FOR CONTROL WITH ORGANIZATION-DEFINED PARAMETER: ASSIGNMENT OPERATIONS

Figure 4 provides an example of an assessment procedure for a control, MP-07, that includes assignment operations and a selection operation. Selection operations include a list of potential parameter values that the organization chooses from and instructions to select one or more parameters. The list of parameter values is identified using braces { }, with each potential parameter value separated with a semicolon. When the ODP for a selection operation is referenced in a subsequent determination statement, the ODP unique identifier and phrase "SELECTED PARAMETER VALUE(S)" is surrounded by < >.

MP-07	MEDIA USE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-07_ODP[01]	***types of system media to be restricted or prohibited from use on systems or system components are defined;***
	MP-07_ODP[02]	***one of the following PARAMETER VALUES is selected to be applied on specific types of system media: {restrict; prohibit};***
	MP-07_ODP[03]	***systems or system components on which the use of specific types of system media to be restricted or prohibited are defined;***
	MP-07_ODP[04]	***controls to restrict or prohibit the use of specific types of system media on systems or system components are defined;***
	MP-07a.	the use of ***<MP-07_ODP[01] types of system media>*** is ***<MP-07_ODP[02] SELECTED PARAMETER VALUE>*** on ***systems or system components>*** using ***<MP-07_ODP[04] controls>***
	MP-07b.	the use of portable storage devices in organizational systems is prohibited when such devices have no identifiable owner.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-07-Examine	[SELECT FROM: System media protection policy; system use policy; procedures addressing media usage restrictions; rules of behavior; system design documentation; system configuration settings and associated documentation; audit records; system security plan; other relevant documents or records].
	MP-07-Interview	[SELECT FROM: Organizational personnel with system media use responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	MP-07-Test	[SELECT FROM: Organizational processes for media use; automated mechanisms restricting or prohibiting use of system media on systems or system components].

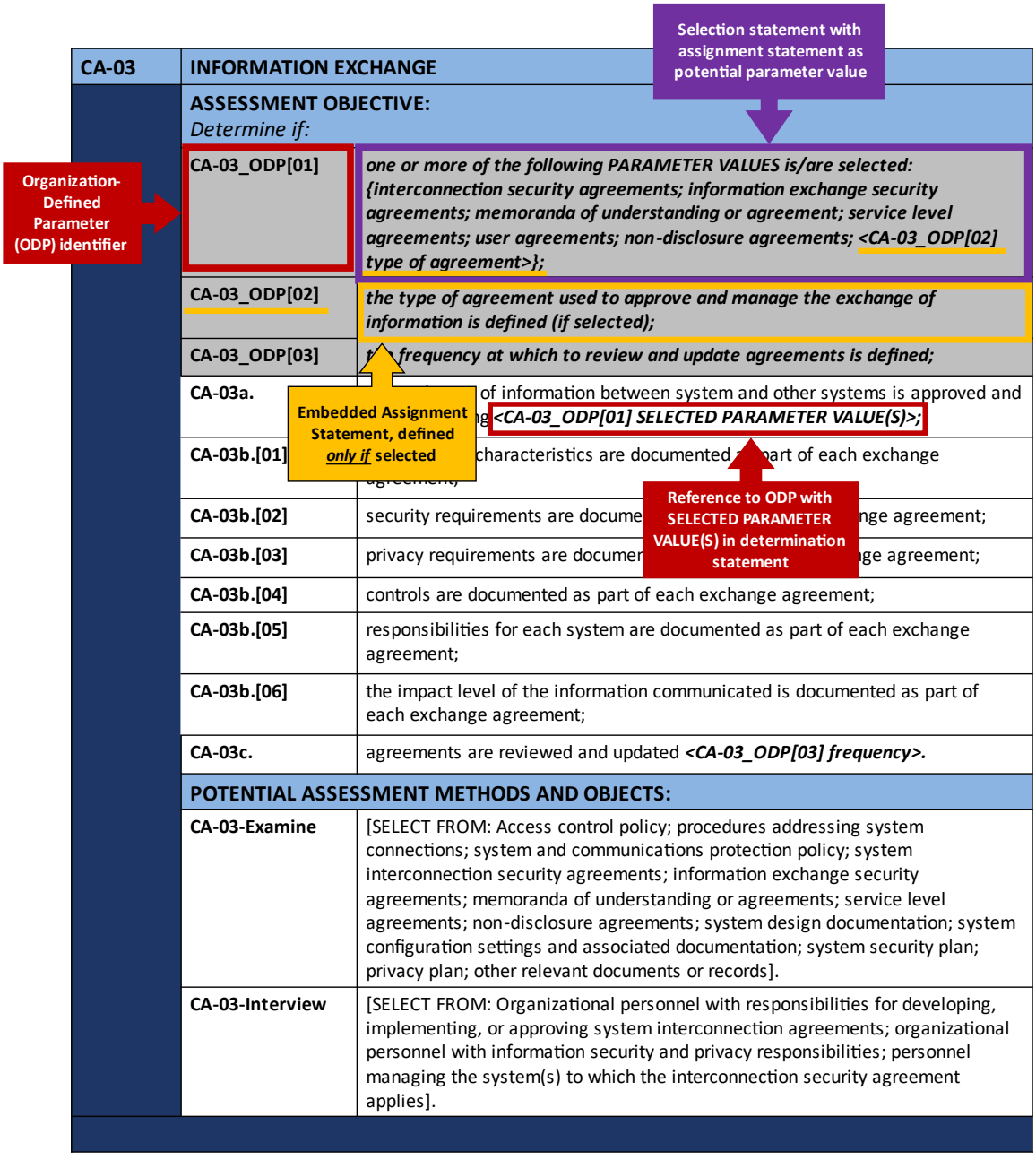
Organization-Defined Parameter (ODP) identifier

Selection Statement

Reference to ODP in determination statement

FIGURE 4. ASSESSMENT PROCEDURE FOR CONTROL WITH ORGANIZATION-DEFINED PARAMETER: SELECTION OPERATION

Figure 5 provides an example of an assessment procedure for a control, CA-03, that includes an ODP that consists of a selection operation with an embedded assignment operation. The selection operation, CA-03(01)_ODP[01], identifies a list of parameters to choose from, including another ODP. The assignment operation for CA-03(01)_ODP[02] is only defined if the organization selects the ODP from the list of parameters. When the ODP for a selection operation is referenced in a subsequent determination statement, the ODP unique identifier and phrase "SELECTED PARAMETER VALUE(S)" is surrounded by < >. In this scenario, if the embedded assignment operation is selected, it becomes the "SELECTED PARAMETER VALUE(S)".



CA-03	INFORMATION EXCHANGE
	ASSESSMENT OBJECTIVE: *Determine if:*
	CA-03_ODP[01] ***one or more of the following PARAMETER VALUES is/are selected: {interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; non-disclosure agreements; <CA-03_ODP[02] type of agreement>};***
	CA-03_ODP[02] ***the type of agreement used to approve and manage the exchange of information is defined (if selected);***
	CA-03_ODP[03] ***the frequency at which to review and update agreements is defined;***
	CA-03a. of information between system and other systems is approved and g ***<CA-03_ODP[01] SELECTED PARAMETER VALUE(S)>;***
	CA-03b.[01] characteristics are documented as part of each exchange agreement;
	CA-03b.[02] security requirements are docume nge agreement;
	CA-03b.[03] privacy requirements are documen ge agreement;
	CA-03b.[04] controls are documented as part of each exchange agreement;
	CA-03b.[05] responsibilities for each system are documented as part of each exchange agreement;
	CA-03b.[06] the impact level of the information communicated is documented as part of each exchange agreement;
	CA-03c. agreements are reviewed and updated ***<CA-03_ODP[03] frequency>.***
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:
	CA-03-Examine [SELECT FROM: Access control policy; procedures addressing system connections; system and communications protection policy; system interconnection security agreements; information exchange security agreements; memoranda of understanding or agreements; service level agreements; non-disclosure agreements; system design documentation; system configuration settings and associated documentation; system security plan; privacy plan; other relevant documents or records].
	CA-03-Interview [SELECT FROM: Organizational personnel with responsibilities for developing, implementing, or approving system interconnection agreements; organizational personnel with information security and privacy responsibilities; personnel managing the system(s) to which the interconnection security agreement applies].

FIGURE 5. ASSESSMENT PROCEDURE FOR CONTROL WITH ORGANIZATION-DEFINED PARAMETERS: SELECTION OPERATION WITH EMBEDDED ASSIGNMENT OPERATION

Although not explicitly noted with each assessment method in the assessment procedure, the attribute values of depth and coverage[26] are assigned by the organization and specified within the assessment plan (e.g., the level of rigor for documentation review, the number of similar assessment objects to test). The assessor/assessment team applies the depth and coverage attributes in the execution of the assessment method against an assessment object to provide the level of assurance required by the organization.

If the control has any enhancements as designated by sequential parenthetical numbers (for example, AC-17(01) for the first enhancement for AC-17), assessment objectives are developed for each enhancement using the same process used for the base control. The resulting assessment objectives are numbered sequentially in the same way as the assessment procedure for the base control – first in accordance with the numbering scheme in [SP 800-53] and, subsequently, using bracketed sequential numbers to further apportion control enhancement requirements to facilitate assessments (e.g., AC-17(01), AC-17(02), AC-17(03)).

Figure 6 illustrates an example of an assessment procedure developed to assess the effectiveness of the first enhancement to security control AC-17, AC-17(01).

AC-17(01)	**REMOTE ACCESS | MONITORING AND CONTROL**	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-17(01)[01]	automated mechanisms are employed to monitor remote access methods;
	AC-17(01)[02]	automated mechanisms are employed to control remote access methods.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-17(01)-Examine	[SELECT FROM: Access control policy; procedures addressing remote access to the system; system design documentation; system configuration settings and associated documentation; system audit records; system monitoring records; system security plan; other relevant documents or records].
	AC-17(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-17(01)-Test	[SELECT FROM: Automated mechanisms monitoring and controlling remote access methods].

FIGURE 6: ASSESSMENT PROCEDURE FOR CONTROL ENHANCEMENT

[26] Attribute values of depth and coverage are described in Appendix C.

CHAPTER THREE

THE PROCESS

CONDUCTING EFFECTIVE SECURITY AND PRIVACY CONTROL ASSESSMENTS

This chapter describes the process of assessing the security and privacy controls in organizational systems and environments of operation. The process to assess controls includes:

- the activities carried out by organizations and assessors to prepare for security and privacy control assessments;
- the development of security and privacy assessment plans; the conduct of control assessments and the analysis, documentation, and reporting of assessment results; and
- post-assessment report analysis and follow-on activities.

Additionally, this chapter describes assessing security and privacy *capabilities*.[27]

FIGURE 7. OVERVIEW OF PROCESS TO CONDUCT EFFECTIVE SECURITY AND PRIVACY CONTROL ASSESSMENTS

3.1 PREPARE FOR SECURITY AND PRIVACY CONTROL ASSESSMENTS

Table 1 provides a summary of the purpose, roles, and expected outcomes of the Prepare for Security and Privacy Control Assessments Step.

TABLE 1. PREPARE FOR SECURITY AND PRIVACY CONTROL ASSESSMENTS SUMMARY

Purpose	**Address a range of issues pertaining to the cost, schedule, scope, and performance of the control assessment.**
Primary Roles	Authorizing Official, Authorizing Official Designated Representative, system owner, common control provider, control assessors
Supporting Roles	System security officer, system privacy officer
Outcomes	• The objective, scope, and timeframe of control assessment determined • Key organizational stakeholders notified and necessary resources allocated • Assessors/assessment teams identified • Artifacts collected and provided to assessors/assessment teams • Mechanism to minimize ambiguities and misunderstandings about control implementation and identified control deficiencies or weaknesses established • Assessors/assessment teams understand the organization's operations, structure, objective, scope, and timeframe of control assessment

[27] A security and privacy *capability* is a combination of mutually reinforcing security and privacy controls (i.e., safeguards and countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals).

Conducting security and privacy control assessments can be difficult, challenging, and resource intensive. Security and privacy control assessments may be conducted by different organizational entities with distinct oversight responsibilities. However, success requires the cooperation and collaboration of all parties with a vested interest in the organization's information security or privacy posture, including control assessors, system security and privacy officers, system owners, common control providers, authorizing officials, chief information officers, senior information security officers, senior agency officials for privacy/chief privacy officers, chief executive officers/heads of agencies, security and privacy staffs, Inspectors General, and OMB. Establishing an appropriate set of expectations before, during, and after an assessment is paramount to achieving an acceptable outcome (i.e., producing information necessary to help the authorizing official make a credible, risk-based decision on whether to place the system into operation or continue its operation).

Thorough preparation by the organization and assessors is an important aspect of conducting effective security and privacy control assessments. Preparatory activities address a range of issues relating to the cost, schedule, and performance of the assessment. From an organizational perspective, preparing for a security and privacy control assessment includes the following key activities:

- Ensuring that appropriate policies covering security and privacy control assessments are in place and understood by all affected organizational elements;
- Ensuring that all steps in the RMF prior to the security or privacy control assessment step have been successfully completed and received appropriate management oversight;[28]
- Establishing the objective and scope of assessments (i.e., the purpose of the assessments and what is being assessed);
- Ensuring that security and privacy controls identified as common controls (and the common portion of hybrid controls) have been assigned to appropriate organizational entities (i.e., common control providers) for development and implementation;[29]
- Notifying key organizational officials of impending assessments and allocating necessary resources to carry out the assessments;
- Establishing appropriate communication channels among organizational officials with an interest in the assessments;
- Establishing time frames for completing the assessments and key milestone decision points required by the organization;
- Identifying and selecting appropriate assessors/assessment teams that will be responsible for conducting the assessments and considering issues of assessor independence;

[28] Conducting security and privacy control assessments in parallel with the development/acquisition and implementation phases of the life cycle allows for the early identification of weaknesses and deficiencies and provides the most cost-effective method for initiating corrective actions. Issues found during development assessments can be referred to authorizing officials for early resolution, as appropriate. The results of security and privacy control assessments carried out during system development and implementation can also be used (consistent with reuse criteria) during the authorization process to avoid system fielding delays or the costly repetition of assessments.

[29] Common control assessments and assessments of the common part of hybrid controls are the responsibility of the common control providers, not the system owner inheriting the controls.

- Providing artifacts to the assessors/assessment teams (e.g., policies, procedures, plans, specifications, designs, records, administrator/operator manuals, system documentation, information exchange agreements, previous assessment results, legal requirements); and
- Establishing a mechanism between the organization and the assessors and/or assessment teams to minimize ambiguities or misunderstandings about the implementation of security and privacy controls and related weaknesses or deficiencies identified during the assessments.

Control assessors/assessment teams begin preparing for their respective assessments by:

- Obtaining a general understanding of the organization's operations (including mission, functions, and business processes) and how the system or common control that is the subject of the particular assessment supports those organizational operations,
- Obtaining an understanding of the structure of the system (i.e., system architecture) and the security and privacy controls being assessed (including system-specific, hybrid, and common controls),
- Identifying the organizational entities responsible for the development and implementation of the common controls (or the common portion of hybrid controls) supporting the system,
- Meeting with appropriate organizational officials to ensure common understanding for assessment objectives and the proposed rigor and scope of the assessment,
- Obtaining artifacts needed for the assessment (e.g., policies, procedures, plans, specifications, designs, records, administrator and operator manuals, system documentation, information exchange agreements, previous assessment results),
- Establishing appropriate organizational points of contact to carry out the assessments, and
- Obtaining previous assessment results that may be appropriately reused for the current assessment (e.g., Inspector General reports, audits, vulnerability scans, physical security inspections, developmental testing and evaluation, vendor flaw remediation activities, [ISO 15408] evaluations).

In preparation for the assessment of security and privacy controls, the necessary background information is assembled and made available to the assessors or assessment team.[30] To the extent necessary to support the specific assessment, and depending upon whether security controls or privacy controls are being assessed, the organization identifies and arranges access to elements of the organization responsible for developing, documenting, disseminating, reviewing, and updating:

- all policies and associated procedures for implementing policy-compliant controls;
- the policies for the system and any associated implementing procedures, individuals, or groups responsible for the development, implementation, operation, and maintenance of controls;

[30] System (or program) owners and organizational entities developing, implementing, and/or administering common controls (i.e., common control providers) are responsible for providing needed information to assessors.

- any artifacts or materials (e.g., security or privacy plans, records, schedules, assessment reports, after-action reports, agreements, authorization packages) associated with the implementation and operation of the controls to be assessed; and
- the specific objects to be assessed.[31]

The availability of essential documentation as well as access to key organizational personnel and the system or common control being assessed are paramount to a successful assessment.

Organizations consider both the technical expertise and level of independence required in selecting security and privacy control assessors.[32] Organizations ensure that assessors possess the required skills and technical expertise to successfully carry out assessments of system-specific, hybrid, and common controls.[33] Skills and expertise includes knowledge of and experience with the specific hardware, software, and firmware components employed by the organization. An independent assessor is any individual capable of conducting an impartial assessment of security and privacy controls employed within or inherited by a system. Impartiality implies that security and privacy control assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management of the system or the determination of security and privacy control effectiveness.[34] The authorizing official or designated representative determines the required level of independence for assessors based on the results of the security categorization process for the system (in the case of security control assessments) and the risk to organizational operations and assets, individuals, other organizations, and the Nation. The authorizing official determines whether the level of assessor independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a risk-based decision on whether to place the system or common control into operation or continue its operation.

Independent security and privacy control assessment services can be obtained from other elements within the organization or be contracted to a public or private sector entity outside of the organization. In special situations (e.g., when the organization that owns the system or common control is small or the organizational structure requires that the security or privacy control assessment be accomplished by individuals who are in the developmental, operational, and/or management chain of the system owner), independence in the assessment process can be achieved by ensuring that the assessment results are carefully reviewed and analyzed by an

[31] In situations where there are multiple security and privacy assessments ongoing or planned within an organization, access to organizational elements, individuals, and artifacts supporting the assessments is centrally managed by the organization to ensure a cost-effective use of time and resources.

[32] In accordance with [OMB A-130], an independent evaluation of the privacy program and practices is not required. However, an organization may choose to employ independent privacy assessments at its discretion.

[33] NIST [SP 800-181] describes the Workforce Framework for Cybersecurity (National Initiative for Cybersecurity Education [NICE] Framework), a fundamental reference for describing and sharing information about cybersecurity work through Task statements, and Knowledge and Skills Statements. The NICE Framework is a reference source with which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of cybersecurity education, training, and workforce development.

[34] Contracted assessment services are considered independent if the system (or program) owner is not directly involved in the contracting process or cannot unduly influence the independence of the assessor(s) conducting the assessment of the security or privacy controls.

independent team of experts to validate the completeness, consistency, and veracity of the results.[35]

3.2 DEVELOP SECURITY AND PRIVACY ASSESSMENT PLANS

Table 2 provides a summary of the purpose, roles, and expected outcomes of the Develop Security and Privacy Assessment Plans Step.

TABLE 2. DEVELOP SECURITY AND PRIVACY PLANS SUMMARY

Purpose	**Provide the objectives for the security and privacy control assessments, as well as a detailed roadmap of how to conduct such assessments based on the security and privacy plan(s).**
Primary Roles	Control assessors
Supporting Roles	System security officers, system privacy officers, system owners
Outcomes	• Controls and control enhancements to be included in assessments are determined • Assessment procedures are selected and tailored; additional procedures for security and privacy requirements/controls not covered by [SP 800-53] are developed • Assessment procedures are optimized to reduce duplication of effort • Assessment plan is finalized, and organizational approval is obtained

The *security assessment plan* and *privacy assessment plan* provide the objectives for the security and privacy control assessments, respectively, as well as a detailed roadmap of how to conduct such assessments. The assessment plans may be developed as one integrated plan or as distinct plans, depending upon organizational needs. The following steps are considered by assessors when developing plans to assess the security and privacy controls in organizational systems or common controls available for inheritance:

- Determine which security and privacy controls/control enhancements are to be included in assessments based on the contents of the security plan and privacy plan (or equivalent document if the controls to be assessed are non-system-based common controls)[36] and the purpose and scope of the assessments,
- Select the appropriate assessment procedures to be used during assessments based on the security or privacy controls and control enhancements to be assessed,
- Tailor the selected assessment procedures (e.g., select appropriate assessment methods and objects, and assign depth and coverage attribute values),
- Develop additional assessment procedures to address any security requirements or controls that are not covered by [SP 800-53],

[35] The authorizing official consults with the Office of the Inspector General, the senior information security officer, senior agency officials for privacy/chief privacy officers, and the chief information officer, as appropriate, to discuss the implications of any decisions on assessor independence in the types of special circumstances described above.

[36] The approach to developing assessment plans and conducting control assessments also applies to information security program plans and privacy program plans.

- Optimize the assessment procedures to reduce duplication of effort (e.g., sequencing and consolidating assessment procedures) and provide cost-effective assessment solutions, and
- Finalize assessment plans and obtain the necessary approvals to execute the plans.

3.2.1 DETERMINE WHICH SECURITY AND PRIVACY CONTROLS ARE TO BE ASSESSED

The security plan and privacy plan provide an overview of the security and privacy requirements for the system and organization and describe the security controls and privacy controls in place or planned for meeting those requirements. For the assessment of common controls that are not implemented by a system, a document equivalent to the security or privacy plan may be used. The assessor starts with the security or privacy controls described in the security or privacy plan and considers the purpose of the assessment. A security or privacy control assessment can be a complete assessment of all controls in a system (e.g., during an initial system authorization process), a partial assessment of the controls in a system (e.g., during system development as part of a targeted assessment resulting from changes affecting specific controls or where controls were previously assessed and the results accepted in the reciprocity process), or a common control assessment.

For partial assessments, system owners and common control providers collaborate with organizational officials with an interest in the assessment (e.g., senior information security officers, senior agency officials for privacy/chief privacy officers, mission/information owners, Inspectors General, and authorizing officials) to determine which controls are to be assessed. The determination of the controls to be assessed depends on the purpose of the assessment. For example, during the initial phases of the system development life cycle, specific controls may be selected for assessment to promote the early detection of weakness and deficiencies and a more cost-effective approach to risk response. After the initial authorization to operate has been granted, targeted assessments may be necessary when changes are made to the system, specific security or privacy controls, common controls, or the environment of operation. In such cases, the focus of the assessment is on the controls that may have been affected by the change.

3.2.2 SELECT PROCEDURES TO ASSESS THE SECURITY AND PRIVACY CONTROLS

SP 800-53A provides assessment procedures for each security and privacy control and control enhancement in [SP 800-53]. For each control in the security plan and privacy plan to be included in the assessment, assessors select the corresponding assessment procedure from Chapter 4. The selected assessment procedures can vary from assessment to assessment based on the current content of the security plans and privacy plans and the purpose of the assessment (e.g., complete assessment, partial assessment, common control assessment).

3.2.3 TAILOR ASSESSMENT PROCEDURES

In a manner similar to how the controls from [SP 800-53] are tailored for the organization's mission, business functions, characteristics of the system, and operating environment, organizations tailor the assessment procedures in Chapter 4 to meet specific organizational needs. Organizations have the flexibility to perform the tailoring process at the organization level for all systems or common controls, at the individual system level, or using a combination of organization-level and system-specific approaches. Control assessors determine if the

organization provides additional tailoring guidance prior to initiating the tailoring process. Assessment procedures are tailored by:

- Selecting the appropriate assessment methods and objects needed to satisfy the stated assessment objectives,
- Selecting the appropriate depth and coverage attribute values to define the rigor and scope of the assessment,
- Identifying common controls and inherited portions of hybrid controls that have been assessed by a separately documented security assessment plan or privacy assessment plan and do not require the repeated execution of the assessment procedures,[37]
- Developing system/platform-specific and organization-specific assessment procedures (which may be adaptations of those in Chapter 4),
- Incorporating assessment results from previous assessments where the results are deemed applicable, and
- Making appropriate adjustments in assessment procedures to obtain the requisite assessment evidence from external providers.

3.2.3.1 ASSESSMENT METHOD- AND OBJECT-RELATED CONSIDERATIONS

Organizations can specify, document, and configure their systems in a variety of ways, and the content and applicability of existing assessment evidence varies. This variety may result in the need to apply a mixture of assessment methods to assessment objects to generate the assessment evidence needed to determine whether the security and privacy controls are effective in their application. Additionally, as described in Section 2.3 and Section 2.4, the number and type of assessment methods and assessment objects needed to provide the required assurance varies based on the depth and coverage needed for the assessment. Therefore, the assessment methods and objects provided with each assessment procedure are termed *potential* to reflect the need to choose the specific methods and objects most appropriate for a specific assessment. The assessment methods and objects chosen are those deemed necessary to produce the evidence needed to make the determinations described in the determination statements in support of assurance requirements and the associated management of risk. The potential methods and objects in the assessment procedure are provided as a resource to assist in the selection of appropriate methods and objects and not with the intent of limiting the selection. Organizations use their judgment when selecting assessment methods and associated assessment objects. Organizations select those methods and objects that most cost-effectively manage risk and contribute to making the determinations associated with the assessment objective.[38] The quality of assessment results is based on the soundness of the rationale provided for selecting the methods and objects, not the specific set

[37] Common controls are not assessed as part of system control assessments unless the common controls are part of a system that provides the common control(s) for inheritance by other systems. The assessor simply verifies that the system being assessed has actually inherited the common control (i.e., that a given inherited common control is being used by the system being assessed to provide protection) and the control is not implemented at the level of the system being assessed.

[38] The selection of assessment methods and objects (including the number and type of assessment objects, i.e., coverage) can be a significant factor in cost-effectively managing risk while still meeting the assessment objectives.

of methods and objects applied. It is not necessary, in most cases, to apply every assessment method to every assessment object to obtain the desired assurance.

3.2.3.2 DEPTH- AND COVERAGE-RELATED CONSIDERATIONS

In addition to selecting appropriate assessment methods and objects, each assessment method (i.e., examine, interview, and test) is associated with the depth and coverage attributes described in Appendix C. The attribute values identify the rigor (depth) and scope (coverage) of the assessment procedures executed by the assessor. The values selected by the organization are based on the characteristics of the system being assessed (including assurance requirements) and the specific determinations to be made. The depth and coverage attribute values are associated with the assurance requirements specified by the organization (i.e., the rigor and scope of the assessment increases in direct relationship with the assurance requirements, which in turn increase in direct relationship with the adverse impact of loss).

3.2.3.3 COMMON CONTROL-RELATED CONSIDERATIONS

Assessors note which security and privacy controls (or parts of such controls) in security plans or privacy plans are designated as *common controls*.[39] Since the assessment of common controls is the responsibility of the organizational entity that developed and implemented the controls (i.e., common control provider), the assessment procedures in Chapter 4 are also used to assess common controls. The results from the common control assessment are made available to organizational systems and system owners that elect to inherit the common controls.[40]

Another consideration in assessing common controls is awareness of system-specific aspects of a control that are not covered by the organizational entities responsible for the common aspects of the control. Such controls are referred to as *hybrid controls*. For example, CP-02, the contingency planning security control, may be considered a hybrid control by the organization if there is a contingency plan developed by the organization for all organizational systems. System owners are expected to adjust or tailor the organization-developed contingency plan when there are specific aspects of the plan that need to be defined for the particular system where the control is employed. For each hybrid control, assessors include in security assessment plans or privacy assessment plans the portions of the assessment procedures from Chapter 4 related to the parts of the control that are system-specific to ensure that, along with the results from common control assessments, all aspects of the control are assessed.

[39] Common controls support multiple systems within the organization, and the protection measures provided by common controls are inherited by individual systems. Therefore, the organization determines the appropriate set of common controls to ensure that both the strength of the controls (i.e., security or privacy capability) and level of rigor and intensity of the control assessments are commensurate with the privacy risk assessment and categorization of the individual systems inheriting those controls. Weaknesses or deficiencies in common controls have the potential to adversely affect large portions of the organization and thus require significant attention.

[40] If assessment results are not currently available for the common controls, the assessment plans for the systems under assessment that depend on those controls are duly noted. The assessments cannot be considered complete until the assessment results for the common controls are made available to system owners.

ASSESSING COMMON CONTROLS AND PORTIONS OF HYBRID CONTROLS INHERITED FROM A COMMON CONTROL PROVIDER

In system security and privacy plans, common controls or portions of hybrid controls implemented and maintained by the common control provider are indicated as "inherited" with a reference to the common control provider. The system owner is not responsible for assessing common controls or the inherited portion of hybrid controls. Common controls are assessed separately and are not reassessed at the system level by each system that inherits them. However, the assessor verifies if the system does, in fact, inherit and utilize the common control as indicated in the system security plans and privacy plans. The assessment of common controls (for the common control provider) is carried out using the same process as a system control assessment.

3.2.3.4 SYSTEM/PLATFORM- AND ORGANIZATION-RELATED CONSIDERATIONS

The assessment procedures in SP 800-53A may be adapted to address system-, platform-, or organization-specific dependencies. For example, the assessment of a Linux implementation of control IA-02 for the identification and authentication of users might include an explicit examination of any key-based, "password-less" login capability and potential risks inherent from any deficiency in key management, account management, system and boundary protection, physical and environmental protection, and other safeguards to prevent identification and authentication bypass by unauthorized users or processes acting on behalf of users.

3.2.3.5 REUSE OF ASSESSMENT EVIDENCE-RELATED CONSIDERATIONS

Reuse of assessment results from previously accepted or approved assessments is considered in the body of evidence for determining overall security and privacy control effectiveness. Previously accepted or approved assessments include assessments of inherited common controls that are managed by the organization and support multiple systems, assessments of security or privacy controls that are reviewed as part of the control implementation (e.g., CP-02 requires a review of the contingency plan), or security-related information generated by the organization's ISCM program. The acceptability of reusing assessment results in a security control assessment or privacy control assessment is coordinated with and approved by the users of the assessment results. It is essential that system owners and common control providers collaborate with authorizing officials and other appropriate organizational officials to determine the acceptability of using previous assessment results. When considering the reuse of assessment results and the value of those results to the current assessment, assessors determine the credibility of the assessment evidence, the appropriateness of previous analysis, and the applicability of the assessment evidence to current system operating conditions. If previous assessment results are reused, the date and type of the original assessment are documented in the assessment plan and assessment report.

In certain situations, it may be necessary to supplement previous assessment results under consideration for reuse with additional assessment activities to fully address the current assessment objectives. For example, if an independent evaluation of an information technology product did not test a particular configuration setting that is employed by the organization in a system, then the assessor may need to supplement the original test results with additional testing to cover that configuration setting for the current system environment. The decision to reuse assessment results is documented in the security assessment plan or privacy assessment

plan and the final security assessment report or privacy assessment report, and it is consistent with legislation, policies, directives, standards, and guidelines.

The following items are considered when validating previous assessment results for reuse:

- **Changing conditions associated with security controls and privacy controls over time.** Security and privacy controls that were deemed effective during previous assessments may have become ineffective due to changing conditions within the system or its environment of operation, including emergent threat information. Assessment results that were found to be previously acceptable may no longer provide credible evidence for the determination of security or privacy control effectiveness, and therefore, a reassessment may be required. Applying previous assessment results to a current assessment necessitates the identification of any changes that have occurred since the previous assessment and the impact of these changes on the previous results. For example, reusing previous assessment results from examining an organization's security or privacy policies and procedures may be acceptable if it is determined that there have not been any significant changes to the identified policies and procedures. Reusing assessment results produced during the previous authorization of a system is a cost-effective method for supporting continuous monitoring activities and annual FISMA reporting requirements when the related controls have not changed and there are adequate reasons for confidence in their continued application.
- **Amount of time that has transpired since previous assessments.** In general, as the time between current and previous assessments increases, the credibility and utility of the previous assessment results decrease. This is primarily because the system or the environment in which the system operates is more likely to change with the passage of time, possibly invalidating the original conditions or assumptions on which the previous assessment was based.
- **Degree of independence of previous assessments.** Assessor independence can be a critical factor in certain types of assessments. The degree of independence required from assessment to assessment should be consistent. For example, it is not appropriate to reuse results from a previous self-assessment where no assessor independence was required when a current assessment requires a greater degree of independence.

3.2.3.6 EXTERNAL SYSTEM- RELATED CONSIDERATIONS

The assessment procedures in Chapter 4 need to be adjusted, as appropriate, to accommodate the assessment of external systems.[41] Because the organization does not always have direct control over the security or privacy controls used in external systems or sufficient visibility into the development, implementation, and assessment of those controls, alternative assessment approaches may need to be applied, resulting in the need to tailor the assessment procedures described in Chapter 4. Where required assurances of agreed-upon security or privacy controls within a system are documented in contracts or service-level agreements, assessors review the contracts or agreements and tailor the assessment procedures as appropriate to assess the

[41] An external system is a system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security and privacy controls or the assessment of control effectiveness. [SP 800-37] and [SP 800-53] provide additional guidance on external systems and the effect of employing security and privacy controls in external environments.

security or privacy controls or the security and privacy control assessment results provided through contracts or agreements. In addition, assessors consider any other assessments that have been conducted or are in the process of being conducted for external systems that are relied upon with regard to protecting the system under assessment. Applicable information from these assessments, if deemed reliable, is incorporated into the security assessment report or privacy assessment report, as appropriate.

3.2.4 DEVELOP ASSESSMENT PROCEDURES FOR ORGANIZATION-SPECIFIC CONTROLS

Based on organizational policies, mission or business function requirements, and an assessment of risk, organizations may choose to develop and implement additional (organization-specific) controls or control enhancements for their systems that are beyond the scope of [SP 800-53]. Such controls are documented in the security plan and privacy plan as controls not found in SP 800-53. To assess the controls not found in SP 800-53, assessors use the guidelines in Chapter 2 to develop assessment procedures for those controls and control enhancements. The assessment procedures developed are subsequently integrated into the assessment plan, as appropriate.

3.2.5 OPTIMIZE SELECTED ASSESSMENT PROCEDURES TO ENSURE MAXIMUM EFFICIENCY

Assessors have flexibility in organizing assessment plans that meet the needs of the organization and that provide the best opportunity for obtaining the necessary evidence to determine security or privacy control effectiveness while reducing overall assessment costs. Combining and consolidating assessment procedures is one area where flexibility can be applied. During the assessment of a system, assessment methods are applied numerous times to a variety of assessment objects within a particular family of controls. To save time, reduce assessment costs, and maximize the usefulness of assessment results, assessors review the selected assessment procedures for the control families and combine or consolidate the procedures (or parts of procedures) whenever possible or practicable. For example, assessors may consolidate interviews with key organizational officials who deal with a variety of security- or privacy-related topics. Assessors may have other opportunities for significant consolidation and cost savings by examining all policies and procedures from the families of security controls and privacy controls at the same time or by organizing groups of related policies and procedures that could be examined as a unified entity. Obtaining and examining configuration settings from similar hardware and software components within the system is another example that can provide significant assessment efficiencies.

An additional area for consideration in optimizing the assessment process is the sequence in which controls are assessed. The assessment of some controls before others may provide useful information that facilitates understanding and more efficient assessments of other controls. For example, controls such as CM-2 (Baseline Configuration), CM-8 (System Component Inventory), PL-2 (System Security and Privacy Plans), RA-2 (Security Categorization), and RA-3 (Risk Assessment) produce general descriptions of the system. Assessing related controls early in the assessment process may provide a basic understanding of the system that can aid in assessing other controls. In SP 800-53, the discussion section for each control identifies related controls that can provide useful information for organizing the assessment procedures. For example, AC-19 (Access Control for Mobile Devices) lists controls MP-4 (Media Storage) and MP-5 (Media Transport) as being related to AC-19. Since AC-19 is related to MP-4 and MP-5, the sequence in

which assessments are conducted for AC-19, MP-4, and MP-5 may facilitate the reuse of assessment information from one control in assessing other related controls.

3.2.6 FINALIZE ASSESSMENT PLAN AND OBTAIN APPROVAL TO EXECUTE PLAN

After selecting the assessment procedures (including developing necessary procedures not contained in the SP 800-53A catalog of procedures), tailoring the procedures for system/platform-specific and organization-specific conditions, optimizing the procedures for efficiency, and addressing the potential for unexpected events that may impact the assessment, the assessment plan is finalized and the schedule is established, including key milestones for the assessment process. Once the assessment plan is completed, the plan is reviewed and approved by appropriate organizational officials[42] to ensure that the plan is complete, consistent with the security and privacy objectives of the organization and the organization's assessment of risk, and cost-effectively manages risk with regard assessment methods and objects, depth and coverage attributes, and to the resources allocated for the assessment.

3.3 CONDUCT SECURITY AND PRIVACY CONTROL ASSESSMENTS

Table 3 provides a summary of the purpose, roles, and expected outcomes of the Conduct Security and Privacy Control Assessments Step.

TABLE 3. CONDUCT SECURITY AND PRIVACY CONTROL ASSESSMENTS SUMMARY

Purpose	**Conduct the security and privacy control assessment in accordance with the assessment plan, and document the results in security and privacy assessment report(s).**
Primary Roles	Control assessors
Supporting Roles	System security and privacy officers, system owners, security and privacy engineers, security and privacy architects, system administrators, system users
Outcomes	• In-scope controls and control enhancements are assessed in accordance with the security and privacy assessment plan(s) • Security and privacy assessment report(s) documenting the effectiveness of the controls and identified weaknesses/deficiencies are produced

After the assessment plan is approved by the organization, the assessor(s) or assessment team executes the plan in accordance with the agreed-upon schedule. Determining the size and organizational makeup of the assessment team (i.e., skill sets, technical expertise, and assessment experience of the individuals composing the team) is one of the risk management decisions made by the organization requesting and initiating the assessment. The results of control assessments are documented in assessment reports, which are key inputs in the authorization package developed by system owners and common control providers for

[42] Organizations establish a security and privacy assessment plan approval process with the specific organizational officials (e.g., systems owners, common control providers, system security and privacy officers, senior information security officers, senior agency officials for privacy/chief privacy officers, authorizing officials) designated as approving authorities.

authorizing officials.[43] Assessment reports include information from assessors (in the form of assessment findings) that is necessary to determine the effectiveness of the security and privacy controls employed within the system.[44] Assessment reports are an important factor in an authorizing official's determination of risk. Organizations may choose to develop an assessment summary from the detailed findings that are generated by assessors during the security control assessments and privacy control assessments. An assessment summary can provide an authorizing official with an abbreviated version of an assessment report that focuses on the highlights of the assessment, synopsis of key findings, and recommendations for addressing weaknesses and deficiencies in the security or privacy controls assessed. Appendix E provides information on the recommended content of assessment reports.

Assessment objectives are achieved by applying the designated assessment methods to selected assessment objects and compiling or producing the evidence necessary to make the determination associated with each assessment objective. Each determination statement[45] contained within an assessment procedure executed by an assessor produces one of the following findings:

- *satisfied (S);* or
- *other than satisfied (O).*

A finding of "satisfied" indicates that – for the portion of the control addressed by the determination statement – the assessment objective for the control has been met and produces a fully acceptable result.

A finding of "other than satisfied" indicates – for the portion of the control addressed by the determination statement – potential anomalies in the operation or implementation of the control that may need to be addressed by the organization. A finding of "other than satisfied" may also indicate that the assessor was unable to obtain sufficient information to make the determination called for in the determination statement for reasons specified in the assessment report. For assessment findings that are "other than satisfied", organizations may choose to define subcategories of findings indicating the severity and/or criticality of the weaknesses or deficiencies discovered and the potential adverse effects on organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. Defining such subcategories can help to establish priorities for needed risk mitigation actions.

Assessor findings are an unbiased, factual reporting of what was found concerning the control assessed. For each finding of "other than satisfied", assessors indicate which parts of the control are affected by the finding (i.e., aspects of the control that were deemed not satisfied or were not able to be assessed) and describe how the actual state of the control differs from the planned or expected/desired state. The potential for compromises to confidentiality, integrity,

[43] In accordance with [SP 800-37], the authorization package consists of the security plan, privacy plan, security assessment report, privacy assessment report, and plan of action and milestones (POA&M).

[44] See Section 3.2.3 for additional information about assessing common controls and portions of hybrid controls inherited from a common control provider.

[45] For additional information on determination statements and assessment findings, see Appendix E.

and availability or privacy risks due to "other than satisfied" findings are also noted by the assessor in the assessment report.

Risk determination and acceptance activities are conducted by the organization post-assessment as part of the risk management strategy established by the organization. Post-assessment risk management activities involve the senior leadership of the organization, such as heads of agencies, mission and business owners, information owners/stewards, risk executive (function), and authorizing officials in consultation with appropriate organizational support staff (e.g., senior information security officers, senior agency officials for privacy/chief privacy officers, chief information officers, system owners, common control providers, and assessors). Security control assessment and privacy control assessment results are documented at a level of detail appropriate for the assessment in accordance with the reporting format prescribed by organizational policy, NIST guidelines, and OMB policy. The reporting format is appropriate for the type of assessment conducted (e.g., self-assessments by system owners and common control providers, independent verification and validation, independent assessments supporting the authorization process, automated assessments, or independent audits or inspections).

System owners and common control providers rely on the expertise and technical judgment of assessors to assess the security and privacy controls in the system and inherited by the system and provide recommendations on how to respond to the control assessment results (e.g., accept risk, reject risk, mitigate risk by correcting weaknesses or deficiencies in the controls and reducing or eliminating identified vulnerabilities). The assessment results produced by the assessor (i.e., findings of "satisfied" or "other than satisfied", identification of the parts of the security or privacy control that did not produce a satisfactory result, and a description of resulting potential for compromises to the system or its environment of operation) are provided to system owners and common control providers in the initial security assessment reports and privacy assessment reports. System owners and common control providers may choose to act on selected recommendations of the assessor before the assessment reports are finalized if there are specific opportunities to correct weaknesses or deficiencies in the security or privacy controls or to correct and/or clarify misunderstandings or interpretations of assessment results.[46] Security or privacy controls that are modified, enhanced, or added during this process are reassessed by the assessor prior to the production of the final assessment reports.

3.4 ANALYZE ASSESSMENT REPORT RESULTS

Table 4 provides a summary of the purpose, roles, and expected outcomes of the Analyze Assessment Report Results Step.

[46] The correction of weaknesses or deficiencies in security or privacy controls or carrying out recommendations during the review of the initial security assessment reports or privacy assessment reports by system owners or common control providers are not intended to replace the formal risk response process by the organization, which occurs after the delivery of the final reports. Rather, it provides the system owner or common control provider with an opportunity to address weaknesses or deficiencies that may be quickly corrected. However, in situations where limited resources exist for remediating weaknesses and deficiencies discovered during the security control assessments or privacy control assessments, organizations may decide without prejudice that waiting for the risk assessment to prioritize remediation efforts is the better course of action.

TABLE 4. ANALYZE ASSESSMENT REPORT RESULTS SUMMARY

Purpose	Analyze the risks resulting from identified weaknesses and deficiencies in controls and determine an approach to respond to risk in accordance with organizational priorities.
Primary Roles	System owners or common control providers, authorizing officials
Supporting Roles	System security and privacy officers, security and privacy engineers, security and privacy architects
Outcomes	• Control assessment findings are reviewed • Subsequent risk responses are taken to manage risk • Authorization package artifacts (e.g., security and privacy plans, security and privacy assessment reports, and plans of action and milestones) are updated to reflect the as-implemented state of the system or common controls

The results of control assessments ultimately influence control implementations, the content of security plans and privacy plans, and the respective plans of action and milestones. Accordingly, system owners and common control providers review the security assessment reports, privacy assessment reports, and updated risk assessment documentation and artifacts and – with the concurrence of designated organizational officials (e.g., authorizing officials, chief information officer, senior information security officer, senior agency officials for privacy/chief privacy officers, mission/information owners) – determine the appropriate steps required to respond to those weaknesses and deficiencies identified during the assessment. By using the labels of "satisfied" and "other than satisfied", the reporting format for the assessment findings provides organizational officials with visibility into specific weaknesses and deficiencies in security or privacy controls within the system or inherited by the system and facilitates a disciplined and structured approach to responding to risks in accordance with organizational priorities. For example, system owners or common control providers in consultation with designated organizational officials may decide that certain assessment findings marked as "other than satisfied" present no significant risk to the organization and can be accepted. Conversely, system owners or common control providers may decide that certain findings marked as "other than satisfied" are significant and require remediation actions. In all cases, the organization reviews each assessment finding of "other than satisfied" and applies its judgment with regard to the severity of the finding and whether it is significant enough to warrant further investigation or remedial action.[47]

Senior leadership involvement in the mitigation process may be necessary to ensure that the organization's resources are effectively allocated in accordance with organizational priorities, provide resources first to the systems that support the most critical and sensitive missions for the organization, or correct the deficiencies that pose the greatest degree of risk. Ultimately, the assessment findings and any subsequent response actions (informed by the updated risk assessment) trigger updates to the key artifacts used by authorizing officials to determine the security and privacy risks of the system and its suitability for authorization to operate. The artifacts include security plans and privacy plans, security assessment reports and privacy assessment reports, and the respective plans of action and milestones.

[47] Potential risk response actions include risk acceptance, risk mitigation, risk rejection, and risk transfer/sharing. [SP 800-39] provides guidance on risk response actions from a risk management perspective.

3.5 ASSESS SECURITY AND PRIVACY CAPABILITIES

In accordance with [SP 800-53], organizations may define a set of security and privacy capabilities as a precursor to the security and privacy control selection process. The concept of capability[48] recognizes that the protection of individuals' privacy and information being processed by systems seldom derives from a single security or privacy safeguard or countermeasure. In most cases, such protection results from the selection and implementation of a set of mutually reinforcing security and privacy controls. Each control contributes to the overall organization-defined capability with some controls potentially contributing to a greater degree and other controls contributing to a lesser degree. For example, organizations may wish to define a capability for secure remote authentication. A secure remote authentication capability can be achieved by the implementation of a set of security controls from SP 800-53 (i.e., IA-02(01), IA-02(02), IA-02(08)], and SC-08(01)).

Security and privacy capabilities can address a variety of areas, including technical means, physical means, procedural means, or any combination thereof. By employing the capability concept, organizations can obtain greater visibility into and a better understanding of the relationships (i.e., dependencies) among controls, the effects of specific control failures on organization-defined capabilities, and the potential severity of control weaknesses or deficiencies. However, when specific capabilities are affected by the failure of particular security and privacy controls, the capability approach may add complexity to assessments and necessitate root cause failure analysis to determine which control or controls are contributing to the failure. The greater the number of controls included in an organization-defined capability, the more difficult it may be to ascertain the root cause of failures. There may also be interactions among defined capabilities, which may contribute to the complexity of assessments. If it is found that a control is neither contributing to a defined capability nor to the overall security and privacy of the system, the organization revisits the RMF Select step, tailors the control set, and documents the rationale in the system security plan or privacy plan.

Traditionally, assessments have been conducted on a control-by-control basis and produce results that are characterized as pass (i.e., control satisfied) or fail (i.e., control not satisfied). However, the failure of a single control or, in some cases, the failure of multiple controls may not affect the overall security and privacy capability required by an organization. This is not to say that such controls do not contribute to the security or privacy of the system and/or organization (as defined by the security requirements and privacy requirements during the initiation phase of the system development life cycle) but rather that such controls may not support the particular security or privacy capability. Furthermore, every implemented security and privacy control may not necessarily support or need to support an organization-defined capability.

When organizations employ the concept of capabilities, automated and manual assessments account for all security and privacy controls that comprise the security and privacy capabilities. Assessors are aware of how the controls work together to provide such capabilities. In this way,

[48] A security capability or privacy capability is a combination of mutually reinforcing security controls or privacy controls (i.e., safeguards and countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals).

when assessments identify a failure in a capability, a root cause analysis can be conducted to determine the specific control or controls that are responsible for the failure based on the established relationships among controls. Moreover, employing the broader capability construct allows organizations to assess the severity of vulnerabilities discovered in their systems and organizations and determine if the failure of a particular security control or privacy control (associated with a vulnerability) or the decision not to deploy a certain control during the initial tailoring process (RMF Select step) affects the overall capability needed for mission and business protection. For example, the failure of a security control deemed critical for a particular security capability may be assigned a higher severity rating than a failed control of lesser importance to the capability.

Ultimately, authorization decisions (i.e., risk acceptance decisions) are made based on the degree to which the desired security and privacy capabilities have been effectively achieved and are meeting the security and privacy requirements defined by an organization. Risk-based decisions are directly related to organizational risk tolerance that is defined as part of an organization's risk management strategy.

CAPABILITY-BASED ASSESSMENTS

The grouping of controls into security and privacy capabilities necessitates root cause analyses to determine if the failure of a particular security or privacy capability can be traced to the failure of one or more security or privacy controls based on the established relationships among controls. The structure of the assessment procedures in this publication with the token-level decomposition and labelling of assessment objectives linked to the specific content of security and privacy controls supports such root cause analysis. Thus, assessments of security and privacy controls (defined as part of capabilities) can be tailored based on the guidance in Section 3.2.3 and [SP 800-137] to define the resource expenditures (e.g., frequency and level of effort) associated with such assessments. This additional precision in assessments is essential to supporting the continuous monitoring strategies developed by organizations and the ongoing authorization decisions of senior leaders.

Figure 8 summarizes the security and privacy control assessment process, including the activities carried out before, during, and after the assessment.

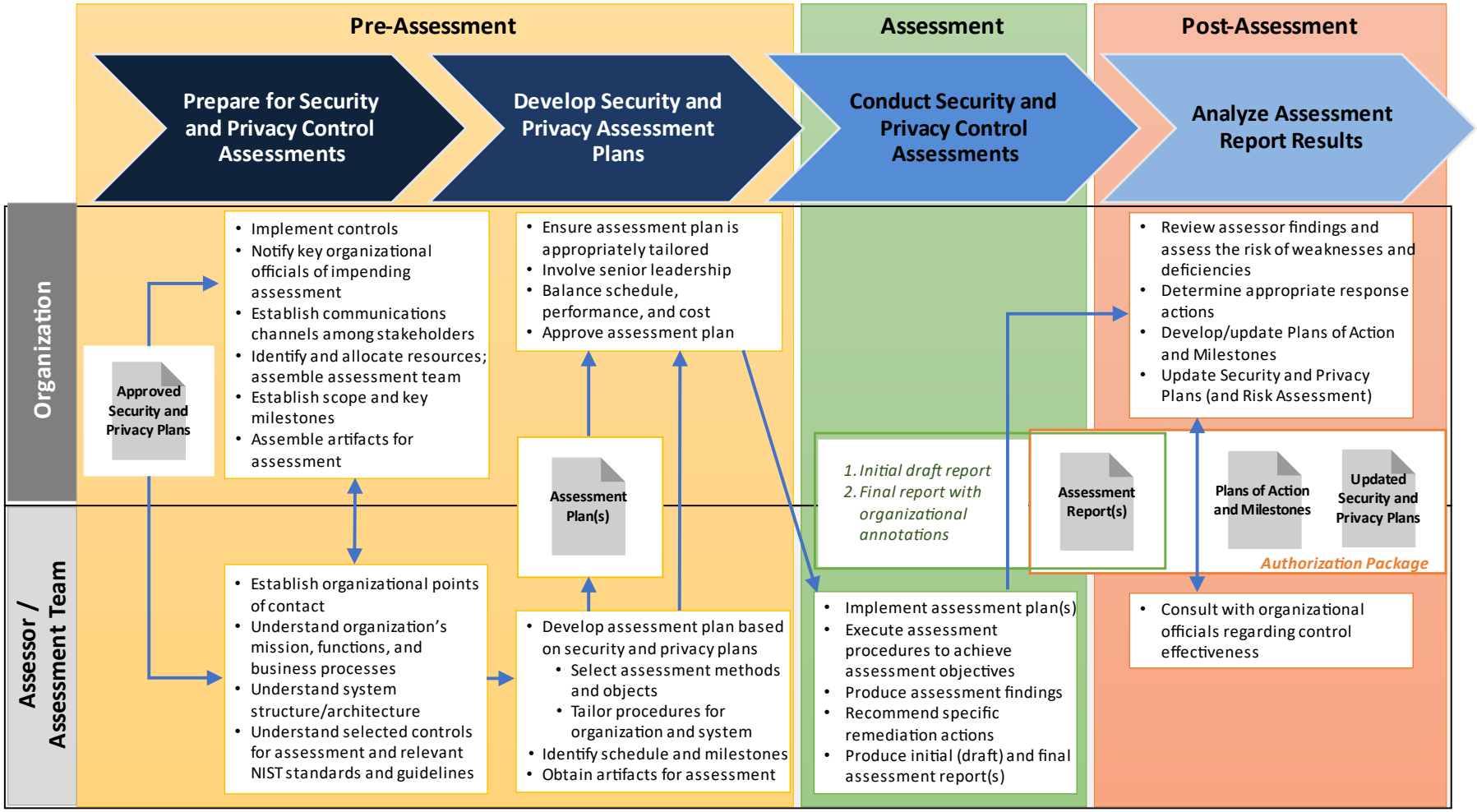


FIGURE 8: SECURITY AND PRIVACY CONTROL ASSESSMENT PROCESS OVERVIEW

CHAPTER FOUR

SECURITY AND PRIVACY ASSESSMENT PROCEDURES

OBJECTIVES, METHODS, AND OBJECTS FOR ASSESSING SECURITY AND PRIVACY CONTROLS

This chapter provides a catalog of procedures to assess the security and privacy controls and control enhancements in [SP 800-53].[49] Assessors select assessment procedures from the catalog in accordance with the guidance provided in Section 3.2. Since the contents of the security and privacy plan are the basis for the development of the security and privacy assessment plans and the assessments, there will likely be assessment procedures in the catalog not used by assessors because the associated security and privacy controls or control enhancements are not contained in the security and privacy plan for the system,[50] or the security and privacy controls or control enhancements are not being assessed at this time.

SP 800-53A REVISION 5, ASSESSMENT PROCEDURE SCHEMA

Section 2.4 provides an overview of the assessment procedures, including the naming and numbering convention, assessment objectives, determination statements, potential assessment methods, and objects.

Appendix C provides definitions of the assessment methods, applicable objects, and additional information on assessment attributes of depth and coverage.

The same assessment object may appear in multiple assessment object lists in a variety of assessment procedures. The same object may be used in multiple contexts to obtain needed information or evidence for a particular aspect of an assessment. Assessors use the general references as appropriate to obtain the necessary information to make the specified determinations required by the assessment objective. For example, a reference to access control policy appears in the assessment procedures for AC-02 and AC-07. For assessment procedure AC-02, assessors use the access control policy to find information about that portion of the policy that addresses account management for the system. For assessment procedure AC-07, assessors use the access control policy to find information about that portion of the policy that addresses unsuccessful login attempts for the system.

Assessors are responsible for combining and consolidating the assessment procedures whenever possible or practical. Optimizing assessment procedures can save time, reduce assessment costs, and maximize the usefulness of assessment results. Assessors optimize assessment procedures by determining the best sequencing of the procedures. The assessment

[49] [SP 800-53] remains the definitive expression of the control or enhancement in the event of any differences between the assessment objectives identified for assessing the security and privacy controls and the underlying intent expressed by the security and privacy control statements defined in the most recent version of SP 800-53.

[50] The execution of the RMF includes the selection of an initial set of security and privacy controls employed within or inherited by an organizational system followed by a control tailoring process. The tailoring process often changes the set of security and privacy controls contained in the final security plan and privacy program plan. Therefore, the selection of assessment procedures from the catalog of available procedures is based solely on the content of the plan(s) after the tailoring activities are completed.

of some security and privacy controls before others may provide information that facilitates understanding and assessment of other controls.[51]

The assessment procedures are published in multiple data formats, including comma-separated values (CSV), plain text, and Open Security Controls Assessment (OSCAL). The available data formats are accessible from on the NIST SP 800-53A Revision 5, publication details page at https://csrc.nist.gov/publications/detail/sp/800-53A/rev-5. The OSCAL Content Git Repository is available at https://github.com/usnistgov/oscal-content.

CAUTIONARY NOTE

Whereas a set of ***potential assessment methods*** are included in the following catalog of assessment procedures, the potential assessment methods are not intended to be mandatory or exclusive. Depending on the particular circumstances of the system or organization to be assessed, not all methods may be required, or other assessment methods may also be used. In addition, the set of ***potential assessment objects*** listed in the catalog are not intended to be mandatory but rather a set from which the necessary and sufficient set of objects for a given assessment can be selected to make the appropriate determinations. Organizational assurance requirements and other risk management-related factors (e.g., system categorization, organizational risk tolerance) are primary drivers for determining the appropriate assessment methods and objects for a given assessment.

[51] For additional information on optimizing assessment procedures, refer to Section 3.2.5.

IMPLEMENTATION TIPS

TIP #1: Select only those assessment procedures from Chapter 4 that correspond to the controls and control enhancements in the approved system security plan and privacy plan to be included in the assessment.

TIP #2: The assessment procedures selected from Chapter 4 are example procedures that serve as a starting point for organizations preparing for assessments. These assessment procedures are tailored as necessary by the assessors in accordance with the guidance in Section 3.2.3 to adapt to specific organizational requirements and operating environments.

TIP #3: With respect to the assessment procedures in Chapter 4, assessors need only apply those procedures, methods, and objects necessary for making a final determination that a particular security control requirement is "satisfied" or "not satisfied" (see Section 3.3).

TIP #4: To each assessment method, assessors apply values for depth and coverage (described in Appendix C) that are commensurate with the characteristics of the system (including assurance requirements) and the specific assessment activity that supports making a determination of the effectiveness of the security controls under review. The values selected for the depth and coverage attributes indicate the relative effort required in applying an assessment method to an assessment object (i.e., the rigor and scope of the activities associated with the assessment). The depth and coverage attributes, while not repeated in every assessment procedure in this appendix, can be represented as follows:

> **Interview:** [assign attribute values: <depth>, <coverage>].
> [SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities].

TIP #5: Assessors may find useful assessment-related information in the Discussion and Related Controls section of each control described in [SP 800-53]. Information from the discussion about related controls can be used to carry out more effective assessments with regard to the application of assessment procedures and the reuse of assessment artifacts.

TIP #6: For controls with ODPs, the ODP values are defined during the RMF Select step and updated as necessary during the RMF Implement and Monitor steps. If ODP values are not defined and implemented, control effectiveness cannot be verified, resulting in an "other than satisfied" finding.

TIP #7: Organizations may refer to this publication or the derivative data formats to easily identify all of the control parameters whose values to define. The ODP definitions are highlighted within the assessment procedure listing and can be filtered using keyword *"_ODP"* or "*XX-nn_ODP*" (where *XX* is the two-character control family abbreviation, and *nn* is the control number).

Note: When assessing agency compliance with NIST guidance, auditors, Inspectors General, evaluators, and/or assessors consider the intent of the security and privacy concepts and principles articulated within the particular guidance document and how the agency applied the guidance in the context of its specific mission responsibilities, operational environments, and unique organizational conditions.

4.1 ACCESS CONTROL

AC-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-01_ODP[01]	***personnel or roles to whom the access control policy is to be disseminated is/are defined;***
	AC-01_ODP[02]	***personnel or roles to whom the access control procedures are to be disseminated is/are defined;***
	AC-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	AC-01_ODP[04]	***an official to manage the access control policy and procedures is defined;***
	AC-01_ODP[05]	***the frequency at which the current access control policy is reviewed and updated is defined;***
	AC-01_ODP[06]	***events that would require the current access control policy to be reviewed and updated are defined;***
	AC-01_ODP[07]	***the frequency at which the current access control procedures are reviewed and updated is defined;***
	AC-01_ODP[08]	***events that would require procedures to be reviewed and updated are defined;***
	AC-01a.[01]	an access control policy is developed and documented;
	AC-01a.[02]	the access control policy is disseminated to ***<AC-01_ODP[01] personnel or roles>***;
	AC-01a.[03]	access control procedures to facilitate the implementation of the access control policy and associated controls are developed and documented;
	AC-01a.[04]	the access control procedures are disseminated to ***<AC-01_ODP[02] personnel or roles>***;
	AC-01a.01(a)[01]	the ***<AC-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** access control policy addresses purpose;
	AC-01a.01(a)[02]	the ***<AC-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** access control policy addresses scope;
	AC-01a.01(a)[03]	the ***<AC-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** access control policy addresses roles;
	AC-01a.01(a)[04]	the ***<AC-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** access control policy addresses responsibilities;
	AC-01a.01(a)[05]	the ***<AC-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** access control policy addresses management commitment;
	AC-01a.01(a)[06]	the ***<AC-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** access control policy addresses coordination among organizational entities;
	AC-01a.01(a)[07]	the ***<AC-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** access control policy addresses compliance;

AC-01	POLICY AND PROCEDURES	
	AC-01a.01(b)	the ***<AC-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** access control policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines;
	AC-01b.	the ***<AC-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the access control policy and procedures;
	AC-01c.01[01]	the current access control policy is reviewed and updated ***<AC-01_ODP[05] frequency>***;
	AC-01c.01[02]	the current access control policy is reviewed and updated following ***<AC-01_ODP[06] events>***;
	AC-01c.02[01]	the current access control procedures are reviewed and updated ***<AC-01_ODP[07] frequency>***;
	AC-01c.02[02]	the current access control procedures are reviewed and updated following ***<AC-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-01-Examine	[SELECT FROM: Access control policy and procedures; system security plan; privacy plan; other relevant documents or records].
	AC-01-Interview	[SELECT FROM: Organizational personnel with access control responsibilities; organizational personnel with information security with information security and privacy responsibilities].

AC-02	ACCOUNT MANAGEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02_ODP[01]	***prerequisites and criteria for group and role membership are defined;***
	AC-02_ODP[02]	***attributes (as required) for each account are defined;***
	AC-02_ODP[03]	***personnel or roles required to approve requests to create accounts is/are defined;***
	AC-02_ODP[04]	***policy, procedures, prerequisites, and criteria for account creation, enabling, modification, disabling, and removal are defined;***
	AC-02_ODP[05]	***personnel or roles to be notified is/are defined;***
	AC-02_ODP[06]	***time period within which to notify account managers when accounts are no longer required is defined;***
	AC-02_ODP[07]	***time period within which to notify account managers when users are terminated or transferred is defined;***
	AC-02_ODP[08]	***time period within which to notify account managers when system usage or the need to know changes for an individual is defined;***
	AC-02_ODP[09]	***attributes needed to authorize system access (as required) are defined;***
	AC-02_ODP[10]	***the frequency of account review is defined;***
	AC-02a.[01]	account types allowed for use within the system are defined and documented;

AC-02	ACCOUNT MANAGEMENT	
	AC-02a.[02]	account types specifically prohibited for use within the system are defined and documented;
	AC-02b.	account managers are assigned;
	AC-02c.	***<AC-02_ODP[01] prerequisites and criteria>*** for group and role membership are required;
	AC-02d.01	authorized users of the system are specified;
	AC-02d.02	group and role membership are specified;
	AC-02d.03[01]	access authorizations (i.e., privileges) are specified for each account;
	AC-02d.03[02]	***<AC-02_ODP[02] attributes (as required)>*** are specified for each account;
	AC-02e.	approvals are required by ***<AC-02_ODP[03] personnel or roles>*** for requests to create accounts;
	AC-02f.[01]	accounts are created in accordance with ***<AC-02_ODP[04] policy, procedures, prerequisites, and criteria>***;
	AC-02f.[02]	accounts are enabled in accordance with ***<AC-02_ODP[04] policy, procedures, prerequisites, and criteria>***;
	AC-02f.[03]	accounts are modified in accordance with ***<AC-02_ODP[04] policy, procedures, prerequisites, and criteria>***;
	AC-02f.[04]	accounts are disabled in accordance with ***<AC-02_ODP[04] policy, procedures, prerequisites, and criteria>***;
	AC-02f.[05]	accounts are removed in accordance with ***<AC-02_ODP[04] policy, procedures, prerequisites, and criteria>***;
	AC-02g.	the use of accounts is monitored;
	AC-02h.01	account managers and ***<AC-02_ODP[05] personnel or roles>*** are notified within ***<AC-02_ODP[06] time period>*** when accounts are no longer required;
	AC-02h.02	account managers and ***<AC-02_ODP[05] personnel or roles>*** are notified within ***<AC-02_ODP[07] time period>*** when users are terminated or transferred;
	AC-02h.03	account managers and ***<AC-02_ODP[05] personnel or roles>*** are notified within ***<AC-02_ODP[08] time period>*** when system usage or the need to know changes for an individual;
	AC-02i.01	access to the system is authorized based on a valid access authorization;
	AC-02i.02	access to the system is authorized based on intended system usage;
	AC-02i.03	access to the system is authorized based on ***<AC-02_ODP[09] attributes (as required)>***;
	AC-02j.	accounts are reviewed for compliance with account management requirements ***<AC-02_ODP[10] frequency>***;
	AC-02k.[01]	a process is established for changing shared or group account authenticators (if deployed) when individuals are removed from the group;
	AC-02k.[02]	a process is implemented for changing shared or group account authenticators (if deployed) when individuals are removed from the group;
	AC-02l.[01]	account management processes are aligned with personnel termination processes;

AC-02	ACCOUNT MANAGEMENT	
	AC-02l.[02]	account management processes are aligned with personnel transfer processes.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-02-Examine	[SELECT FROM: Access control policy; personnel termination policy and procedure; personnel transfer policy and procedure; procedures for addressing account management; system design documentation; system configuration settings and associated documentation; list of active system accounts along with the name of the individual associated with each account; list of recently disabled system accounts and the name of the individual associated with each account; list of conditions for group and role membership; notifications of recent transfers, separations, or terminations of employees; access authorization records; account management compliance reviews; system monitoring records; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-02-Interview	[SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security with information security and privacy responsibilities].
	AC-02-Test	[SELECT FROM: Organizational processes for account management on the system; mechanisms for implementing account management].

AC-02(01)	ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(01)_ODP	***automated mechanisms used to support the management of system accounts are defined;***
	AC-02(01)	the management of system accounts is supported using ***<AC-02(01)_ODP automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-02(01)-Examine	[SELECT FROM: Access control policy; procedures for addressing account management; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-02(01)-Interview	[SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security with information security responsibilities; system developers].
	AC-02(01)-Test	[SELECT FROM: Automated mechanisms for implementing account management functions].

AC-02(02)	ACCOUNT MANAGEMENT | AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(02)_ODP[01]	***one of the following PARAMETER VALUES is selected: {remove; disable};***

AC-02(02)	ACCOUNT MANAGEMENT | AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT	
	AC-02(02)_ODP[02]	***the time period after which to automatically remove or disable temporary or emergency accounts is defined;***
	AC-02(02)	temporary and emergency accounts are automatically ***<AC-02(02)_ODP[01] SELECTED PARAMETER VALUE>*** after ***<AC-02(02)_ODP[02] time period>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-02(02)-Examine	[SELECT FROM: Access control policy; procedures for addressing account management; system design documentation; system configuration settings and associated documentation; system-generated list of temporary accounts removed and/or disabled; system-generated list of emergency accounts removed and/or disabled; system audit records; system security plan; other relevant documents or records].
	AC-02(02)-Interview	[SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security with information security responsibilities; system developers].
	AC-02(02)-Test	[SELECT FROM: Automated mechanisms for implementing account management functions].

AC-02(03)	ACCOUNT MANAGEMENT | DISABLE ACCOUNTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(03)_ODP[01]	***time period within which to disable accounts is defined;***
	AC-02(03)_ODP[02]	***time period for account inactivity before disabling is defined;***
	AC-02(03)(a)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have expired;
	AC-02(03)(b)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts are no longer associated with a user or individual;
	AC-02(03)(c)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts are in violation of organizational policy;
	AC-02(03)(d)	accounts are disabled within ***<AC-02(03)_ODP[01] time period>*** when the accounts have been inactive for ***<AC-02(03)_ODP[02] time period>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-02(03)-Examine	[SELECT FROM: Access control policy; procedures for addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; system-generated list of accounts removed; system-generated list of emergency accounts disabled; system audit records; system security plan; other relevant documents or records].
	AC-02(03)-Interview	[SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-02(03)-Test	[SELECT FROM: Mechanisms for implementing account management functions].

AC-02(04)	ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(04)[01]	account creation is automatically audited;
	AC-02(04)[02]	account modification is automatically audited;
	AC-02(04)[03]	account enabling is automatically audited;
	AC-02(04)[04]	account disabling is automatically audited;
	AC-02(04)[05]	account removal actions are automatically audited.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-02(04)-Examine	[SELECT FROM: Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated documentation; notifications/alerts of account creation, modification, enabling, disabling, and removal actions; system audit records; system security plan; other relevant documents or records].
	AC-02(04)-Interview	[SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-02(04)-Test	[SELECT FROM: Automated mechanisms implementing account management functions].

AC-02(05)	ACCOUNT MANAGEMENT | INACTIVITY LOGOUT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(05)_ODP	***the time period of expected inactivity or description of when to log out is defined;***
	AC-02(05)	users are required to log out when ***<AC-02(05)_ODP time period of expected inactivity or description of when to log out>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-02(05)-Examine	[SELECT FROM: Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated documentation; security violation reports; system audit records; system security plan; other relevant documents or records].
	AC-02(05)-Interview	[SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities; users that must comply with inactivity logout policy].

AC-02(06)	ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(06)_ODP	***dynamic privilege management capabilities are defined;***
	AC-02(06)	***<AC-02(06)_ODP dynamic privilege management capabilities>*** are implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-02(06)-Examine	[SELECT FROM: Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated documentation; system-generated list of dynamic privilege management capabilities; system audit records; system security plan; other relevant documents or records].
	AC-02(06)-Interview	[SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-02(06)-Test	[SELECT FROM: system or mechanisms implementing dynamic privilege management capabilities].

AC-02(07)	ACCOUNT MANAGEMENT | PRIVILEGED USER ACCOUNTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(07)_ODP	***one of the following PARAMETER VALUES is selected: {a role-based access scheme; an attribute-based access scheme};***
	AC-02(07)(a)	privileged user accounts are established and administered in accordance with ***<AC-02(07)_ODP SELECTED PARAMETER VALUE>***;
	AC-02(07)(b)	privileged role or attribute assignments are monitored;
	AC-02(07)(c)	changes to roles or attributes are monitored;
	AC-02(07)(d)	access is revoked when privileged role or attribute assignments are no longer appropriate.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-02(07)-Examine	[SELECT FROM: Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated documentation; system-generated list of privileged user accounts and associated roles; records of actions taken when privileged role assignments are no longer appropriate; system audit records; audit tracking and monitoring reports; system monitoring records; system security plan; other relevant documents or records].
	AC-02(07)-Interview	[SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-02(07)-Test	[SELECT FROM: Mechanisms implementing account management functions; mechanisms monitoring privileged role assignments].

AC-02(08)	ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT MANAGEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(08)_ODP	***system accounts that are dynamically created, activated, managed, and deactivated are defined;***
	AC-02(08)[01]	***<AC-02(08)_ODP system accounts>*** are created dynamically;
	AC-02(08)[02]	***<AC-02(08)_ODP system accounts>*** are activated dynamically;
	AC-02(08)[03]	***<AC-02(08)_ODP system accounts>*** are managed dynamically;
	AC-02(08)[04]	***<AC-02(08)_ODP system accounts>*** are deactivated dynamically.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-02(08)-Examine	[SELECT FROM: Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated documentation; system-generated list of system accounts; system audit records; system security plan; other relevant documents or records].
	AC-02(08)-Interview	[SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-02(08)-Test	[SELECT FROM: Automated mechanisms implementing account management functions].

AC-02(09)	ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED AND GROUP ACCOUNTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(09)_ODP	***conditions for establishing shared and group accounts are defined;***
	AC-02(09)	the use of shared and group accounts is only permitted if ***<AC-02(09)_ODP conditions>*** are met.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-02(09)-Examine	[SELECT FROM: Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated documentation; system-generated list of shared/group accounts and associated roles; system audit records; system security plan; other relevant documents or records].
	AC-02(09)-Interview	[SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-02(09)-Test	[SELECT FROM: Mechanisms implementing management of shared/group accounts].

AC-02(10)	ACCOUNT MANAGEMENT | SHARED AND GROUP ACCOUNT CREDENTIAL CHANGE
	[WITHDRAWN: Incorporated into AC-2k.]

AC-02(11)	ACCOUNT MANAGEMENT | USAGE CONDITIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(11)_ODP[01]	***circumstances and/or usage conditions to be enforced for system accounts are defined;***
	AC-02(11)_ODP[02]	***system accounts subject to enforcement of circumstances and/or usage conditions are defined;***
	AC-02(11)	***<AC-02(11)_ODP[01] circumstances and/or usage conditions>*** for ***<AC-02(11)_ODP[02] system accounts>*** are enforced.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-02(11)-Examine	[SELECT FROM: Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated documentation; system-generated list of system accounts and associated assignments of usage circumstances and/or usage conditions; system audit records; system security plan; other relevant documents or records].
	AC-02(11)-Interview	[SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-02(11)-Test	[SELECT FROM: Mechanisms implementing account management functions].

AC-02(12)	ACCOUNT MANAGEMENT | ACCOUNT MONITORING FOR ATYPICAL USAGE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(12)_ODP[01]	***atypical usage for which to monitor system accounts is defined;***
	AC-02(12)_ODP[02]	***personnel or roles to report atypical usage is/are defined;***
	AC-02(12)(a)	system accounts are monitored for ***<AC-02(12)_ODP[01] atypical usage>***;
	AC-02(12)(b)	atypical usage of system accounts is reported to ***<AC-02(12)_ODP[02] personnel or roles>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-02(12)-Examine	[SELECT FROM: Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated documentation; system monitoring records; system audit records; audit tracking and monitoring reports; privacy impact assessment; system security plan; privacy plan; other relevant documents or records].
	AC-02(12)-Interview	[SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities].

AC-02(12)	ACCOUNT MANAGEMENT | ACCOUNT MONITORING FOR ATYPICAL USAGE	
	AC-02(12)-Test	[SELECT FROM: Mechanisms implementing account management functions].

AC-02(13)	ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-02(13)_ODP[01]	***time period within which to disable accounts of individuals who are discovered to pose significant risk is defined;***
	AC-02(13)_ODP[02]	***significant risks leading to disabling accounts are defined;***
	AC-02(13)	accounts of individuals are disabled within ***<AC-02(13)_ODP[01] time period>*** of discovery of ***<AC-02(13)_ODP[02] significant risks>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-02(13)-Examine	[SELECT FROM: Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated documentation; system-generated list of disabled accounts; list of user activities posing significant organizational risk; system audit records; system security plan; other relevant documents or records].
	AC-02(13)-Interview	[SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-02(13)-Test	[SELECT FROM: Mechanisms implementing account management functions].

AC-03	ACCESS ENFORCEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-03	approved authorizations for logical access to information and system resources are enforced in accordance with applicable access control policies.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-03-Examine	[SELECT FROM: Access control policy; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; list of approved authorizations (user privileges); system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-03-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security and privacy responsibilities; system developers].
	AC-03-Test	[SELECT FROM: Mechanisms implementing access control policy].

AC-03(01)	ACCESS ENFORCEMENT | RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS
	[WITHDRAWN: Incorporated into AC-06.]

AC-03(02)	ACCESS ENFORCEMENT | DUAL AUTHORIZATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-03(02)_ODP	***privileged commands and/or other actions requiring dual authorization are defined;***
	AC-03(02)	dual authorization is enforced for ***<AC-03(02)_ODP privileged commands and/or other actions>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-03(02)-Examine	[SELECT FROM: Access control policy; procedures addressing access enforcement and dual authorization; system design documentation; system configuration settings and associated documentation; list of privileged commands requiring dual authorization; list of actions requiring dual authorization; list of approved authorizations (user privileges); system security plan; other relevant documents or records].
	AC-03(02)-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-03(02)-Test	[SELECT FROM: Dual authorization mechanisms implementing access control policy].

AC-03(03)	ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-03(03)_ODP[01]	***mandatory access control policy enforced over the set of covered subjects is defined;***
	AC-03(03)_ODP[02]	***mandatory access control policy enforced over the set of covered objects is defined;***
	AC-03(03)_ODP[03]	***subjects to be explicitly granted privileges are defined;***
	AC-03(03)_ODP[04]	***privileges to be explicitly granted to subjects are defined;***
	AC-03(03)[01]	***<AC-03(03)_ODP[01] mandatory access control policy>*** is enforced over the set of covered subjects specified in the policy;
	AC-03(03)[02]	***<AC-03(03)_ODP[02] mandatory access control policy>*** is enforced over the set of covered objects specified in the policy;
	AC-03(03)(a)[01]	***<AC-03(03)_ODP[01] mandatory access control policy>*** is uniformly enforced across the covered subjects within the system;
	AC-03(03)(a)[02]	***<AC-03(03)_ODP[02] mandatory access control policy>*** is uniformly enforced across the covered objects within the system;

AC-03(03)	ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL	
	AC-03(03)(b)(01)	***<AC-03(03)_ODP[01] mandatory access control policy>*** and ***<AC-03(03)_ODP[02] mandatory access control policy>*** specifying that a subject that has been granted access to information is constrained from passing the information to unauthorized subjects or objects are enforced;
	AC-03(03)(b)(02)	***<AC-03(03)_ODP[01] mandatory access control policy>*** and ***<AC-03(03)_ODP[02] mandatory access control policy>*** specifying that a subject that has been granted access to information is constrained from granting its privileges to other subjects are enforced;
	AC-03(03)(b)(03)	***<AC-03(03)_ODP[01] mandatory access control policy>*** and ***<AC-03(03)_ODP[02] mandatory access control policy>*** specifying that a subject that has been granted access to information is constrained from changing one of more security attributes (specified by the policy) on subjects, objects, the system, or system components are enforced;
	AC-03(03)(b)(04)	***<AC-03(03)_ODP[01] mandatory access control policy>*** and ***<AC-03(03)_ODP[02] mandatory access control policy>*** specifying that a subject that has been granted access to information is constrained from choosing the security attributes and attribute values (specified by the policy) to be associated with newly created or modified objects are enforced;
	AC-03(03)(b)(05)	***<AC-03(03)_ODP[01] mandatory access control policy>*** and ***<AC-03(03)_ODP[02] mandatory access control policy>*** specifying that a subject that has been granted access to information is constrained from changing the rules governing access control are enforced;
	AC-03(03)(c)	***<AC-03(03)_ODP[01] mandatory access control policy>*** and ***<AC-03(03)_ODP[02] mandatory access control policy>*** specifying that ***<AC-03(03)_ODP[03] subjects>*** may explicitly be granted ***<AC-03(03)_ODP[04] privileges>*** such that they are not limited by any defined subset (or all) of the above constraints are enforced.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-03(03)-Examine	[SELECT FROM: Access control policy; mandatory access control policies; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; list of subjects and objects (i.e., users and resources) requiring enforcement of mandatory access control policies; system audit records; system security plan; other relevant documents or records].
	AC-03(03)-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-03(03)-Test	[SELECT FROM: Automated mechanisms implementing mandatory access control].

AC-03(04)	ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-03(04)_ODP[01]	***discretionary access control policy enforced over the set of covered subjects is defined;***
	AC-03(04)_ODP[02]	***discretionary access control policy enforced over the set of covered objects is defined;***

AC-03(04)	ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL	
	AC-03(04)[01]	***<AC-03(04)_ODP[01] discretionary access control policy>*** is enforced over the set of covered subjects specified in the policy;
	AC-03(04)[02]	***<AC-03(04)_ODP[02] discretionary access control policy>*** is enforced over the set of covered objects specified in the policy;
	AC-03(04)(a)	***<AC-03(04)_ODP[01] discretionary access control policy>*** and ***<AC-03(04)_ODP[02] discretionary access control policy>*** are enforced where the policy specifies that a subject that has been granted access to information can pass the information to any other subjects or objects;
	AC-03(04)(b)	***<AC-03(04)_ODP[01] discretionary access control policy>*** and ***<AC-03(04)_ODP[02] discretionary access control policy>*** are enforced where the policy specifies that a subject that has been granted access to information can grant its privileges to other subjects;
	AC-03(04)(c)	***<AC-03(04)_ODP[01] discretionary access control policy>*** and ***<AC-03(04)_ODP[02] discretionary access control policy>*** are enforced where the policy specifies that a subject that has been granted access to information can change security attributes on subjects, objects, the system, or the system's components;
	AC-03(04)(d)	***<AC-03(04)_ODP[01] discretionary access control policy>*** and ***<AC-03(04)_ODP[02] discretionary access control policy>*** are enforced where the policy specifies that a subject that has been granted access to information can choose the security attributes to be associated with newly created or revised objects;
	AC-03(04)(e)	***<AC-03(04)_ODP[01] discretionary access control policy>*** and ***<AC-03(04)_ODP[02] discretionary access control policy>*** are enforced where the policy specifies that a subject that has been granted access to information can change the rules governing access control.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-03(04)-Examine	[SELECT FROM: Access control policy; discretionary access control policies; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; list of subjects and objects (i.e., users and resources) requiring enforcement of discretionary access control policies; system audit records; system security plan; other relevant documents or records].
	AC-03(04)-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-03(04)-Test	[SELECT FROM: Mechanisms implementing discretionary access control policy].

AC-03(05)	ACCESS ENFORCEMENT | SECURITY-RELEVANT INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-03(05)_ODP	***security-relevant information to which access is prevented except during secure, non-operable system states is defined;***
	AC-03(05)	access to ***<AC-03(05)_ODP security-relevant information>*** is prevented except during secure, non-operable system states.

AC-03(05)	ACCESS ENFORCEMENT | SECURITY-RELEVANT INFORMATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-03(05)-Examine	[SELECT FROM: Access control policy; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-03(05)-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-03(05)-Test	[SELECT FROM: Mechanisms preventing access to security-relevant information within the system].

AC-03(06)	ACCESS ENFORCEMENT | PROTECTION OF USER AND SYSTEM INFORMATION
	[WITHDRAWN: Incorporated into MP-04, SC-28.]

AC-03(07)	ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-03(07)_ODP[01]	***roles upon which to base control of access are defined;***
	AC-03(07)_ODP[02]	***users authorized to assume roles (defined in AC-03(07)_ODP[01]) are defined;***
	AC-03(07)[01]	a role-based access control policy is enforced over defined subjects;
	AC-03(07)[02]	a role-based access control policy is enforced over defined objects;
	AC-03(07)[03]	access is controlled based on ***<AC-03(07)_ODP[01] roles>*** and ***<AC-03(07)_ODP[02] users authorized to assume such roles>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-03(07)-Examine	[SELECT FROM: Access control policy; role-based access control policies; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; list of roles, users, and associated privileges required to control system access; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-03(07)-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security and privacy responsibilities; system developers].
	AC-03(07)-Test	[SELECT FROM: Mechanisms implementing role-based access control policy].

AC-03(08)	ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-03(08)_ODP	***rules governing the timing of revocations of access authorizations are defined;***
	AC-03(08)[01]	revocation of access authorizations is enforced, resulting from changes to the security attributes of subjects based on ***<AC-03(08)_ODP rules>***;
	AC-03(08)[02]	revocation of access authorizations is enforced resulting from changes to the security attributes of objects based on ***<AC-03(08)_ODP rules>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-03(08)-Examine	[SELECT FROM: Access control policy; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; rules governing revocation of access authorizations, system audit records; system security plan; other relevant documents or records].
	AC-03(08)-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-03(08)-Test	[SELECT FROM: Mechanisms implementing access enforcement functions].

AC-03(09)	ACCESS ENFORCEMENT | CONTROLLED RELEASE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-03(09)_ODP[01]	***the outside system or system component to which to release information is defined;***
	AC-03(09)_ODP[02]	***controls to be provided by the outside system or system component (defined in AC-03(09)_ODP[01]) are defined;***
	AC-03(09)_ODP[03]	***controls used to validate appropriateness of information to be released are defined;***
	AC-03(09)(a)	information is released outside of the system only if the receiving ***<AC-03(09)_ODP[01] system or system component>*** provides ***<AC-03(09)_ODP[02] controls>***;
	AC-03(09)(b)	information is released outside of the system only if ***<AC-03(09)_ODP[03] controls>*** are used to validate the appropriateness of the information designated for release.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-03(09)-Examine	[SELECT FROM: Access control policy; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; list of security and privacy safeguards provided by receiving system or system components; list of security and privacy safeguards validating appropriateness of information designated for release; system audit records; results of period assessments (inspections/tests) of the external system; information sharing agreements; memoranda of understanding; acquisitions/ contractual agreements; system security plan; privacy plan; other relevant documents or records].

AC-03(09)	ACCESS ENFORCEMENT | CONTROLLED RELEASE	
	AC-03(09)-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security and privacy responsibilities; organizational personnel with responsibility for acquisitions/contractual agreements; legal counsel; system developers].
	AC-03(09)-Test	[SELECT FROM: Mechanisms implementing access enforcement functions].

AC-03(10)	ACCESS ENFORCEMENT | AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-03(10)_ODP[01]	***conditions under which to employ an audited override of automated access control mechanisms are defined;***
	AC-03(10)_ODP[02]	***roles allowed to employ an audited override of automated access control mechanisms are defined;***
	AC-03(10)	an audited override of automated access control mechanisms is employed under ***<AC-03(10)_ODP[01] conditions>*** by ***<AC-03(10)_ODP[02] roles>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-03(10)-Examine	[SELECT FROM: Access control policy; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; conditions for employing audited override of automated access control mechanisms; system audit records; system security plan; other relevant documents or records].
	AC-03(10)-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-03(10)-Test	[SELECT FROM: Mechanisms implementing access enforcement functions].

AC-03(11)	ACCESS ENFORCEMENT | RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-03(11)_ODP	***information types requiring restricted access to data repositories are defined;***
	AC-03(11)	access to data repositories containing ***<AC-03(11)_ODP information types>*** is restricted.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-03(11)-Examine	[SELECT FROM: Access control policy; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-03(11)-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities; organizational personnel with responsibilities for data repositories; system/network administrators; organizational personnel with information security responsibilities].

AC-03(11)	ACCESS ENFORCEMENT | RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES	
	AC-03(11)-Test	[SELECT FROM: Mechanisms implementing access enforcement functions].

AC-03(12)	ACCESS ENFORCEMENT | ASSERT AND ENFORCE APPLICATION ACCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-03(12)_ODP	***system applications and functions requiring access assertion are defined;***
	AC-03(12)(a)	as part of the installation process, applications are required to assert the access needed to the following system applications and functions: ***<AC-03(12)_ODP system applications and functions>***;
	AC-03(12)(b)	an enforcement mechanism to prevent unauthorized access is provided;
	AC-03(12)(c)	access changes after initial installation of the application are approved.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-03(12)-Examine	[SELECT FROM: Access control policy; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-03(12)-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-03(12)-Test	[SELECT FROM: Mechanisms implementing access enforcement functions].

AC-03(13)	ACCESS ENFORCEMENT | ATTRIBUTE-BASED ACCESS CONTROL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-03(13)_ODP	***attributes to assume access permissions are defined;***
	AC-03(13)[01]	the attribute-based access control policy is enforced over defined subjects;
	AC-03(13)[02]	the attribute-based access control policy is enforced over defined objects;
	AC-03(13)[03]	access is controlled based on ***<AC-03(13)_ODP attributes>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-03(13)-Examine	[SELECT FROM: Access control policy; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; list of subjects and objects (i.e., users and resources) requiring enforcement of attribute-based access control policies; system audit records; system security plan; other relevant documents or records].
	AC-03(13)-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities].

AC-03(13)	ACCESS ENFORCEMENT | ATTRIBUTE-BASED ACCESS CONTROL	
	AC-03(13)-Test	[SELECT FROM: Mechanisms implementing access enforcement functions].

AC-03(14)	ACCESS ENFORCEMENT | INDIVIDUAL ACCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-03(14)_ODP[01]	***mechanisms enabling individuals to have access to elements of their personally identifiable information are defined;***
	AC-03(14)_ODP[02]	***elements of personally identifiable information to which individuals have access are defined;***
	AC-03(14)	***<AC-03(14)_ODP[01] mechanisms>*** are provided to enable individuals to have access to ***<AC-03(14)_ODP[02] elements>*** of their personally identifiable information.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-03(14)-Examine	[SELECT FROM: Access mechanisms (e.g., request forms and application interfaces); access control policy; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; documentation regarding access to an individual's personally identifiable information; system audit records; system security plan; privacy plan; privacy impact assessment; privacy assessment findings and/or reports; other relevant documents or records].
	AC-03(14)-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security and privacy responsibilities; legal counsel].
	AC-03(14)-Test	[SELECT FROM: Mechanisms implementing access enforcement functions; mechanisms enabling individual access to personally identifiable information].

AC-03(15)	ACCESS ENFORCEMENT | DISCRETIONARY AND MANDATORY ACCESS CONTROL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-03(15)_ODP[01]	***a mandatory access control policy enforced over the set of covered subjects specified in the policy is defined;***
	AC-03(15)_ODP[02]	***a mandatory access control policy enforced over the set of covered objects specified in the policy is defined;***
	AC-03(15)_ODP[03]	***a discretionary access control policy enforced over the set of covered subjects specified in the policy is defined;***
	AC-03(15)_ODP[04]	***a discretionary access control policy enforced over the set of covered objects specified in the policy is defined;***
	AC-03(15)(a)[01]	***<AC-03(15)_ODP[01] mandatory access control policy>*** is enforced over the set of covered subjects specified in the policy;

AC-03(15)	ACCESS ENFORCEMENT | DISCRETIONARY AND MANDATORY ACCESS CONTROL	
	AC-03(15)(a)[02]	***<AC-03(15)_ODP[02] mandatory access control policy>*** is enforced over the set of covered objects specified in the policy;
	AC-03(15)(b)[01]	***<AC-03(15)_ODP[03] discretionary access control policy>*** is enforced over the set of covered subjects specified in the policy;
	AC-03(15)(b)[02]	***<AC-03(15)_ODP[04] discretionary access control policy>*** is enforced over the set of covered objects specified in the policy.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-03(15)-Examine	[SELECT FROM: Access control policy; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; list of subjects and objects (i.e., users and resources) requiring enforcement of mandatory access control policies; list of subjects and objects (i.e., users and resources) requiring enforcement of discretionary access control policies; system audit records; system security plan; other relevant documents or records].
	AC-03(15)-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-03(15)-Test	[SELECT FROM: Mechanisms implementing mandatory and discretionary access control policy].

AC-04	INFORMATION FLOW ENFORCEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04_ODP	***information flow control policies within the system and between connected systems are defined;***
	AC-04	approved authorizations are enforced for controlling the flow of information within the system and between connected systems based on ***<AC-04_ODP information flow control policies>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04-Examine	[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; security architecture documentation; privacy architecture documentation; system design documentation; system configuration settings and associated documentation; system baseline configuration; list of information flow authorizations; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-04-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy architecture development responsibilities; organizational personnel with information security and privacy responsibilities; system developers].
	AC-04-Test	[SELECT FROM: Mechanisms implementing information flow enforcement policy].

AC-04(01)	INFORMATION FLOW ENFORCEMENT | OBJECT SECURITY AND PRIVACY ATTRIBUTES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(01)_ODP[01]	***security attributes to be associated with information, source, and destination objects are defined;***
	AC-04(01)_ODP[02]	***privacy attributes to be associated with information, source, and destination objects are defined;***
	AC-04(01)_ODP[03]	***information objects to be associated with information security attributes are defined;***
	AC-04(01)_ODP[04]	***information objects to be associated with privacy attributes are defined;***
	AC-04(01)_ODP[05]	***source objects to be associated with information security attributes are defined;***
	AC-04(01)_ODP[06]	***source objects to be associated with privacy attributes are defined;***
	AC-04(01)_ODP[07]	***destination objects to be associated with information security attributes are defined;***
	AC-04(01)_ODP[08]	***destination objects to be associated with privacy attributes are defined;***
	AC-04(01)_ODP[09]	***information flow control policies as a basis for enforcement of flow control decisions are defined;***
	AC-04(01)[01]	***<AC-04(01)_ODP[01] security attributes>*** associated with ***<AC-04(01)_ODP[03] information objects>***, ***<AC-04(01)_ODP[05] source objects>*** , and ***<AC-04(01)_ODP[07] destination objects>*** are used to enforce ***<AC-04(01)_ODP[09] information flow control policies>*** as a basis for flow control decisions;
	AC-04(01)[02]	***<AC-04(01)_ODP[02] privacy attributes>*** associated with ***<AC-04(01)_ODP[04] information objects>***, ***<AC-04(01)_ODP[06] source objects>*** , and ***<AC-04(01)_ODP[08] destination objects>*** are used to enforce ***<AC-04(01)_ODP[09] information flow control policies>*** as a basis for flow control decisions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(01)-Examine	[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; list of security and privacy attributes and associated source and destination objects; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-04(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with privacy responsibilities; system developers].
	AC-04(01)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement policy].

AC-04(02)	INFORMATION FLOW ENFORCEMENT | PROCESSING DOMAINS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(02)_ODP	***information flow control policies to be enforced by use of protected processing domains are defined;***
	AC-04(02)	protected processing domains are used to enforce ***<AC-04(02)_ODP information flow control policies>*** as a basis for flow control decisions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(02)-Examine	[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system security architecture and associated documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-04(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	AC-04(02)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement policy].

AC-04(03)	INFORMATION FLOW ENFORCEMENT | DYNAMIC INFORMATION FLOW CONTROL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(03)_ODP	***information flow control policies to be enforced are defined;***
	AC-04(03)	***<AC-04(03)_ODP information flow control policies>*** are enforced.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(03)-Examine	[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system security architecture and associated documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-04(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-04(03)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement policy].

AC-04(04)	INFORMATION FLOW ENFORCEMENT | FLOW CONTROL OF ENCRYPTED INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(04)_ODP[01]	***information flow control mechanisms that encrypted information is prevented from bypassing are defined;***

AC-04(04)	INFORMATION FLOW ENFORCEMENT | FLOW CONTROL OF ENCRYPTED INFORMATION	
	AC-04(04)_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; <AC-04(04)_ODP[03] organization-defined procedure or method>};***
	AC-04(04)_ODP[03]	***the organization-defined procedure or method used to prevent encrypted information from bypassing information flow control mechanisms is defined (if selected);***
	AC-04(04)	encrypted information is prevented from bypassing ***<AC-04(04)_ODP[01] information flow control mechanisms>*** by ***<AC-04(04)_ODP[02] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(04)-Examine	[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-04(04)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-04(04)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement policy].

AC-04(05)	INFORMATION FLOW ENFORCEMENT | EMBEDDED DATA TYPES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(05)_ODP	***limitations on embedding data types within other data types are defined;***
	AC-04(05)	***<AC-04(05)_ODP limitations>*** are enforced on embedding data types within other data types.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(05)-Examine	[SELECT FROM: Access control policy; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; list of limitations to be enforced on embedding data types within other data types; system audit records; system security plan; other relevant documents or records].
	AC-04(05)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-04(05)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement policy].

AC-04(06)	INFORMATION FLOW ENFORCEMENT | METADATA	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(06)_ODP	***metadata on which to base enforcement of information flow control is defined;***

AC-04(06)	INFORMATION FLOW ENFORCEMENT | METADATA	
	AC-04(06)	information flow control enforcement is based on ***<AC-04(06)_ODP metadata>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(06)-Examine	[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; types of metadata used to enforce information flow control decisions; system audit records; system security plan; other relevant documents or records].
	AC-04(06)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-04(06)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement policy].

AC-04(07)	INFORMATION FLOW ENFORCEMENT | ONE-WAY FLOW MECHANISMS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(07)	one-way information flows are enforced through hardware-based flow control mechanisms.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(07)-Examine	[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; system hardware mechanisms and associated configurations; system audit records; system security plan; other relevant documents or records].
	AC-04(07)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-04(07)-Test	[SELECT FROM: Hardware mechanisms implementing information flow enforcement policy].

AC-04(08)	INFORMATION FLOW ENFORCEMENT | SECURITY AND PRIVACY POLICY FILTERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(08)_ODP[01]	***security policy filters to be used as a basis for enforcing information flow control are defined;***
	AC-04(08)_ODP[02]	***privacy policy filters to be used as a basis for enforcing information flow control are defined;***
	AC-04(08)_ODP[03]	***information flows for which information flow control is enforced by security filters are defined;***
	AC-04(08)_ODP[04]	***information flows for which information flow control is enforced by privacy filters are defined;***

AC-04(08)	INFORMATION FLOW ENFORCEMENT | SECURITY AND PRIVACY POLICY FILTERS	
	AC-04(08)_ODP[05]	***one or more of the following PARAMETER VALUES is/are selected: {block; strip; modify; quarantine};***
	AC-04(08)_ODP[06]	***security policy identifying actions to be taken after a filter processing failure are defined;***
	AC-04(08)_ODP[07]	***privacy policy identifying actions to be taken after a filter processing failure are defined;***
	AC-04(08)(a)[01]	information flow control is enforced using ***<AC-04(08)_ODP[01] security policy filter>*** as a basis for flow control decisions for ***<AC-04(08)_ODP[03] information flows>***;
	AC-04(08)(a)[02]	information flow control is enforced using ***<AC-04(08)_ODP[02] privacy policy filter>*** as a basis for flow control decisions for ***<AC-04(08)_ODP[04] information flows>***;
	AC-04(08)(b)	***<AC-04(08)_ODP[05] SELECTED PARAMETER VALUE(S)>*** data after a filter processing failure in accordance with ***<AC-04(08)_ODP[06] security policy>***; ***<AC-04(08)_ODP[05] SELECTED PARAMETER VALUE(S)>*** data after a filter processing failure in accordance with ***<AC-04(08)_ODP[07] privacy policy>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(08)-Examine	[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; list of security policy filters regulating flow control decisions; list of privacy policy filters regulating flow control decisions; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-04(08)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; system developers].
	AC-04(08)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement policy; security and privacy policy filters].

AC-04(09)	INFORMATION FLOW ENFORCEMENT | HUMAN REVIEWS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(09)_ODP[01]	***information flows requiring the use of human reviews are defined;***
	AC-04(09)_ODP[02]	***conditions under which the use of human reviews for information flows are to be enforced are defined;***
	AC-04(09)	human reviews are used for ***<AC-04(09)_ODP[01] information flows>*** under ***<AC-04(09)_ODP[02] conditions>***.

AC-04(09)	INFORMATION FLOW ENFORCEMENT | HUMAN REVIEWS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(09)-Examine	[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; records of human reviews regarding information flows; list of information flows requiring the use of human reviews; list of conditions requiring human reviews for information flows; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-04(09)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; organizational personnel with information flow enforcement responsibilities; system developers].
	AC-04(09)-Test	[SELECT FROM: Mechanisms enforcing the use of human reviews].

AC-04(10)	INFORMATION FLOW ENFORCEMENT | ENABLE AND DISABLE SECURITY OR PRIVACY POLICY FILTERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(10)_ODP[01]	***security policy filters that privileged administrators have the capability to enable and disable are defined;***
	AC-04(10)_ODP[02]	***privacy policy filters that privileged administrators have the capability to enable and disable are defined;***
	AC-04(10)_ODP[03]	***conditions under which privileged administrators have the capability to enable and disable security policy filters are defined;***
	AC-04(10)_ODP[04]	***conditions under which privileged administrators have the capability to enable and disable privacy policy filters are defined;***
	AC-04(10)[01]	capability is provided for privileged administrators to enable and disable ***<AC-04(10)_ODP[01] security filters>*** under ***<AC-04(10)_ODP[03] conditions>***;
	AC-04(10)[02]	capability is provided for privileged administrators to enable and disable ***<AC-04(10)_ODP[02] privacy filters>*** under ***<AC-04(10)_ODP[04] conditions>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(10)-Examine	[SELECT FROM: Access control policy; information flow information policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; list of security policy filters enabled/disabled by privileged administrators; list of privacy policy filters enabled/disabled by privileged administrators; list of approved data types for enabling/disabling by privileged administrators; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-04(10)-Interview	[SELECT FROM: Organizational personnel with responsibilities for enabling/disabling security and privacy policy filters; system/network administrators; organizational personnel with information security and privacy responsibilities; system developers].
	AC-04(10)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement policy; security and privacy policy filters].

AC-04(11)	INFORMATION FLOW ENFORCEMENT | CONFIGURATION OF SECURITY OR PRIVACY POLICY FILTERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(11)_ODP[01]	***security policy filters that privileged administrators have the capability to configure to support different security and privacy policies are defined;***
	AC-04(11)_ODP[02]	***privacy policy filters that privileged administrators have the capability to configure to support different security and privacy policies are defined;***
	AC-04(11)[01]	capability is provided for privileged administrators to configure ***<AC-04(11)_ODP[01] security policy filters>*** to support different security or privacy policies;
	AC-04(11)[02]	capability is provided for privileged administrators to configure ***<AC-04(11)_ODP[02] privacy policy filters>*** to support different security or privacy policies.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(11)-Examine	[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; list of security policy filters; list of privacy policy filters; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-04(11)-Interview	[SELECT FROM: Organizational personnel with responsibilities for configuring security and privacy policy filters; system/network administrators; organizational personnel with information security and privacy responsibilities; system developers].
	AC-04(11)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement policy; security and privacy policy filters].

AC-04(12)	INFORMATION FLOW ENFORCEMENT | DATA TYPE IDENTIFIERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(12)_ODP	***data type identifiers to be used to validate data essential for information flow decisions are defined;***
	AC-04(12)	when transferring information between different security domains, ***<AC-04(12)_ODP data type identifiers>*** are used to validate data essential for information flow decisions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(12)-Examine	[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; list of data type identifiers; system audit records; system security plan; other relevant documents or records].
	AC-04(12)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-04(12)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement policy].

AC-04(13)	INFORMATION FLOW ENFORCEMENT | DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(13)_ODP	***policy-relevant subcomponents into which to decompose information for submission to policy enforcement mechanisms are defined;***
	AC-04(13)	when transferring information between different security domains, information is decomposed into ***<AC-04(13)_ODP policy-relevant subcomponents>*** for submission to policy enforcement mechanisms.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(13)-Examine	[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-04(13)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-04(13)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement policy].

AC-04(14)	INFORMATION FLOW ENFORCEMENT | SECURITY OR PRIVACY POLICY FILTER CONSTRAINTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(14)_ODP[01]	***security policy filters to be implemented that require fully enumerated formats restricting data structure and content have been defined;***
	AC-04(14)_ODP[02]	***privacy policy filters to be implemented that require fully enumerated formats restricting data structure and content are defined;***
	AC-04(14)[01]	when transferring information between different security domains, implemented ***<AC-04(14)_ODP[01] security policy filters>*** require fully enumerated formats that restrict data structure and content;
	AC-04(14)[02]	when transferring information between different security domains, implemented ***<AC-04(14)_ODP[02] privacy policy filters>*** require fully enumerated formats that restrict data structure and content.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(14)-Examine	[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; list of security and privacy policy filters; list of data structure policy filters; list of data content policy filters; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-04(14)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; system developers].

AC-04(14)	INFORMATION FLOW ENFORCEMENT | SECURITY OR PRIVACY POLICY FILTER CONSTRAINTS	
	AC-04(14)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement policy; security and privacy policy filters].

AC-04(15)	INFORMATION FLOW ENFORCEMENT | DETECTION OF UNSANCTIONED INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(15)_ODP[01]	***unsanctioned information to be detected is defined;***
	AC-04(15)_ODP[02]	***security policy that requires the transfer of unsanctioned information between different security domains to be prohibited is defined (if selected);***
	AC-04(15)_ODP[03]	***privacy policy that requires the transfer of organization-defined unsanctioned information between different security domains to be prohibited is defined (if selected);***
	AC-04(15)[01]	when transferring information between different security domains, information is examined for the presence of ***<AC-04(15)_ODP[01] unsanctioned information>***;
	AC-04(15)[02]	when transferring information between different security domains, transfer of ***<AC-04(15)_ODP[01] unsanctioned information>*** is prohibited in accordance with the ***<AC-04(15)_ODP[02] security policy>***;
	AC-04(15)[03]	when transferring information between different security domains, transfer of ***<AC-04(15)_ODP[01] unsanctioned information>*** is prohibited in accordance with the ***<AC-04(15)_ODP[03] privacy policy>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(15)-Examine	[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; list of unsanctioned information types and associated information; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-04(15)-Interview	[SELECT FROM: Organizational personnel with information security responsibilities; organizational personnel with privacy responsibilities; system developers].
	AC-04(15)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement policy].

AC-04(16)	INFORMATION FLOW ENFORCEMENT | INFORMATION TRANSFERS ON INTERCONNECTED SYSTEMS
	[WITHDRAWN: Incorporated into AC-04.]

AC-04(17)	INFORMATION FLOW ENFORCEMENT | DOMAIN AUTHENTICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(17)_ODP	***one or more of the following PARAMETER VALUES is/are selected: {organization, system, application, service, individual};***
	AC-04(17)	source and destination points are uniquely identified and authenticated by ***<AC-04(17)_ODP SELECTED PARAMETER VALUE(S)>*** for information transfer.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(17)-Examine	[SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; procedures addressing source and destination domain identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; list of system labels; system security plan; privacy plan; other relevant documents or records].
	AC-04(17)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; system developers].
	AC-04(17)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement policy].

AC-04(18)	INFORMATION FLOW ENFORCEMENT | SECURITY ATTRIBUTE BINDING
	[WITHDRAWN: Incorporated into AC-16.]

AC-04(19)	INFORMATION FLOW ENFORCEMENT | VALIDATION OF METADATA	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(19)_ODP[01]	***security policy filters to be implemented on metadata are defined (if selected);***
	AC-04(19)_ODP[02]	***privacy policy filters to be implemented on metadata are defined (if selected);***
	AC-04(19)[01]	when transferring information between different security domains, ***<AC-04(19)_ODP[01] security policy filters>*** are implemented on metadata;
	AC-04(19)[02]	when transferring information between different security domains, ***<AC-04(19)_ODP[02] privacy policy filters>*** are implemented on metadata.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(19)-Examine	[SELECT FROM: Information flow enforcement policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; list of security policy filtering criteria applied to metadata and data payloads; system audit records; system security plan; privacy plan; other relevant documents or records].

AC-04(19)	INFORMATION FLOW ENFORCEMENT | VALIDATION OF METADATA	
	AC-04(19)-Interview	[SELECT FROM: Organizational personnel with information flow enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; organizational personnel with privacy responsibilities; system developers].
	AC-04(19)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement functions; security and policy filters].

AC-04(20)	INFORMATION FLOW ENFORCEMENT | APPROVED SOLUTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(20)_ODP[01]	***solutions in approved configurations to control the flow of information across security domains are defined;***
	AC-04(20)_ODP[02]	***information to be controlled when it flows across security domains is defined;***
	AC-04(20)	***<AC-04(20)_ODP[01] solutions in approved configurations>*** are employed to control the flow of ***<AC-04(20)_ODP[02] information>*** across security domains.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(20)-Examine	[SELECT FROM: Information flow enforcement policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; list of solutions in approved configurations; approved configuration baselines; system audit records; system security plan; other relevant documents or records].
	AC-04(20)-Interview	[SELECT FROM: Organizational personnel with information flow enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-04(20)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement functions].

AC-04(21)	INFORMATION FLOW ENFORCEMENT | PHYSICAL OR LOGICAL SEPARATION OF INFORMATION FLOWS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(21)_ODP[01]	***mechanisms and/or techniques used to logically separate information flows are defined (if selected);***
	AC-04(21)_ODP[02]	***mechanisms and/or techniques used to physically separate information flows are defined (if selected);***
	AC-04(21)_ODP[03]	***required separations by types of information are defined;***
	AC-04(21)[01]	information flows are separated logically using ***<AC-04(21)_ODP[01] mechanisms and/or techniques>*** to accomplish ***<AC-04(21)_ODP[03] required separations>***;
	AC-04(21)[02]	information flows are separated physically using ***<AC-04(21)_ODP[02] mechanisms and/or techniques>*** to accomplish ***<AC-04(21)_ODP[03] required separations>***.

AC-04(21)	INFORMATION FLOW ENFORCEMENT | PHYSICAL OR LOGICAL SEPARATION OF INFORMATION FLOWS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(21)-Examine	[SELECT FROM: Information flow enforcement policy; information flow control policies; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; list of required separation of information flows by information types; list of mechanisms and/or techniques used to logically or physically separate information flows; system audit records; system security plan; other relevant documents or records].
	AC-04(21)-Interview	[SELECT FROM: Organizational personnel with information flow enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-04(21)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement functions].

AC-04(22)	INFORMATION FLOW ENFORCEMENT | ACCESS ONLY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(22)	access is provided from a single device to computing platforms, applications, or data that reside in multiple different security domains while preventing information flow between the different security domains.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(22)-Examine	[SELECT FROM: Information flow enforcement policy; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-04(22)-Interview	[SELECT FROM: Organizational personnel with information flow enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-04(22)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement functions].

AC-04(23)	INFORMATION FLOW ENFORCEMENT | MODIFY NON-RELEASABLE INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(23)_ODP	***modification action implemented on non-releasable information is defined;***
	AC-04(23)	when transferring information between security domains, non-releasable information is modified by implementing ***<AC-04(23)_ODP modification action>***.

AC-04(23)	INFORMATION FLOW ENFORCEMENT | MODIFY NON-RELEASABLE INFORMATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(23)-Examine	[SELECT FROM: Information flow enforcement policy; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-04(23)-Interview	[SELECT FROM: Organizational personnel with information flow enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-04(23)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement functions].

AC-04(24)	INFORMATION FLOW ENFORCEMENT | INTERNAL NORMALIZED FORMAT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(24)[01]	when transferring information between different security domains, incoming data is parsed into an internal, normalized format;
	AC-04(24)[02]	when transferring information between different security domains, the data is regenerated to be consistent with its intended specification.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(24)-Examine	[SELECT FROM: Information flow enforcement policy; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-04(24)-Interview	[SELECT FROM: Organizational personnel with information flow enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-04(24)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement functions].

AC-04(25)	INFORMATION FLOW ENFORCEMENT | DATA SANITIZATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(25)_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {delivery of malicious content, command and control of malicious code, malicious code augmentation, and steganography-encoded data; spillage of sensitive information};***
	AC-04(25)_ODP[02]	***policy for sanitizing data is defined;***
	AC-04(25)	when transferring information between different security domains, data is sanitized to minimize ***<AC-04(25)_ODP[01] SELECTED PARAMETER VALUE(S)>*** in accordance with ***<AC-04(25)_ODP[02] policy>***.

AC-04(25)	INFORMATION FLOW ENFORCEMENT | DATA SANITIZATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(25)-Examine	[SELECT FROM: Information flow enforcement policy; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-04(25)-Interview	[SELECT FROM: Organizational personnel with information flow enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-04(25)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement functions].

AC-04(26)	INFORMATION FLOW ENFORCEMENT | AUDIT FILTERING ACTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(26)[01]	when transferring information between different security domains, content-filtering actions are recorded and audited;
	AC-04(26)[02]	when transferring information between different security domains, results for the information being filtered are recorded and audited.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(26)-Examine	[SELECT FROM: Information flow enforcement policy; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-04(26)-Interview	[SELECT FROM: Organizational personnel with information flow enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-04(26)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement functions; mechanisms implementing content filtering; mechanisms recording and auditing content filtering].

AC-04(27)	INFORMATION FLOW ENFORCEMENT | REDUNDANT/INDEPENDENT FILTERING MECHANISMS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(27)	when transferring information between security domains, implemented content filtering solutions provide redundant and independent filtering mechanisms for each data type.

AC-04(27)	INFORMATION FLOW ENFORCEMENT | REDUNDANT/INDEPENDENT FILTERING MECHANISMS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(27)-Examine	[SELECT FROM: Information flow enforcement policy; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-04(27)-Interview	[SELECT FROM: Organizational personnel with information flow enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-04(27)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement functions].

AC-04(28)	INFORMATION FLOW ENFORCEMENT | LINEAR FILTER PIPELINES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(28)	when transferring information between security domains, a linear content filter pipeline is implemented that is enforced with discretionary and mandatory access controls.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(28)-Examine	[SELECT FROM: Information flow enforcement policy; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-04(28)-Interview	[SELECT FROM: Organizational personnel with information flow enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-04(28)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement functions; mechanisms implementing linear content filters].

AC-04(29)	INFORMATION FLOW ENFORCEMENT | FILTER ORCHESTRATION ENGINES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(29)_ODP	***policy for content-filtering actions is defined;***
	AC-04(29)(a)	when transferring information between security domains, content filter orchestration engines are employed to ensure that content-filtering mechanisms successfully complete execution without errors;
	AC-04(29)(b)[01]	when transferring information between security domains, content filter orchestration engines are employed to ensure that content-filtering actions occur in the correct order;

AC-04(29)	INFORMATION FLOW ENFORCEMENT | FILTER ORCHESTRATION ENGINES	
	AC-04(29)(b)[02]	when transferring information between security domains, content filter orchestration engines are employed to ensure that content-filtering actions comply with ***<AC-04(29)_ODP policy>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(29)-Examine	[SELECT FROM: Information flow enforcement policy; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-04(29)-Interview	[SELECT FROM: Organizational personnel with information flow enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-04(29)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement functions; mechanisms implementing content filter orchestration engines].

AC-04(30)	INFORMATION FLOW ENFORCEMENT | FILTER MECHANISMS USING MULTIPLE PROCESSES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(30)	when transferring information between security domains, content-filtering mechanisms using multiple processes are implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(30)-Examine	[SELECT FROM: Information flow enforcement policy; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-04(30)-Interview	[SELECT FROM: Organizational personnel with information flow enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-04(30)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement functions; mechanisms implementing content filtering].

AC-04(31)	INFORMATION FLOW ENFORCEMENT | FAILED CONTENT TRANSFER PREVENTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(31)	when transferring information between different security domains, the transfer of failed content to the receiving domain is prevented.

AC-04(31)	INFORMATION FLOW ENFORCEMENT | FAILED CONTENT TRANSFER PREVENTION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(31)-Examine	[SELECT FROM: Information flow enforcement policy; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-04(31)-Interview	[SELECT FROM: Organizational personnel with information flow enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-04(31)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement functions].

AC-04(32)	INFORMATION FLOW ENFORCEMENT | PROCESS REQUIREMENTS FOR INFORMATION TRANSFER	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-04(32)(a)	when transferring information between different security domains, the process that transfers information between filter pipelines does not filter message content;
	AC-04(32)(b)	when transferring information between different security domains, the process that transfers information between filter pipelines validates filtering metadata;
	AC-04(32)(c)	when transferring information between different security domains, the process that transfers information between filter pipelines ensures that the content with the filtering metadata has successfully completed filtering;
	AC-04(32)(d)	when transferring information between different security domains, the process that transfers information between filter pipelines transfers the content to the destination filter pipeline.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-04(32)-Examine	[SELECT FROM: Information flow enforcement policy; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-04(32)-Interview	[SELECT FROM: Organizational personnel with information flow enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-04(32)-Test	[SELECT FROM: Mechanisms implementing information flow enforcement functions; mechanisms implementing content filtering].

AC-05	SEPARATION OF DUTIES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-05_ODP	***duties of individuals requiring separation are defined;***

AC-05	SEPARATION OF DUTIES	
	AC-05a.	***<AC-05_ODP duties of individuals>*** are identified and documented;
	AC-05b.	system access authorizations to support separation of duties are defined.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-05-Examine	[SELECT FROM: Access control policy; procedures addressing divisions of responsibility and separation of duties; system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; system access authorizations; system audit records; system security plan; other relevant documents or records].
	AC-05-Interview	[SELECT FROM: Organizational personnel with responsibilities for defining appropriate divisions of responsibility and separation of duties; organizational personnel with information security responsibilities; system/network administrators].
	AC-05-Test	[SELECT FROM: Mechanisms implementing separation of duties policy].

AC-06	LEAST PRIVILEGE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-06	the principle of least privilege is employed, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-06-Examine	[SELECT FROM: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-06-Interview	[SELECT FROM: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators].
	AC-06-Test	[SELECT FROM: Mechanisms implementing least privilege functions].

AC-06(01)	LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-06(01)_ODP[01]	***individuals and roles with authorized access to security functions and security-relevant information are defined;***
	AC-06(01)_ODP[02]	***security functions (deployed in hardware) for authorized access are defined;***
	AC-06(01)_ODP[03]	***security functions (deployed in software) for authorized access are defined;***
	AC-06(01)_ODP[04]	***security functions (deployed in firmware) for authorized access are defined;***

AC-06(01)	LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS	
	AC-06(01)_ODP[05]	***security-relevant information for authorized access is defined;***
	AC-06(01)(a)[01]	access is authorized for ***<AC-06(01)_ODP[01] individuals and roles>*** to ***<AC-06(01)_ODP[02] security functions (deployed in hardware)>***;
	AC-06(01)(a)[02]	access is authorized for ***<AC-06(01)_ODP[01] individuals and roles>*** to ***<AC-06(01)_ODP[03] security functions (deployed in software)>***;
	AC-06(01)(a)[03]	access is authorized for ***<AC-06(01)_ODP[01] individuals and roles>*** to ***<AC-06(01)_ODP[04] security functions (deployed in firmware)>***;
	AC-06(01)(b)	access is authorized for ***<AC-06(01)_ODP[01] individuals and roles>*** to ***<AC-06(01)_ODP[05] security-relevant information>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-06(01)-Examine	[SELECT FROM: Access control policy; procedures addressing least privilege; list of security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-06(01)-Interview	[SELECT FROM: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators].
	AC-06(01)-Test	[SELECT FROM: Mechanisms implementing least privilege functions].

AC-06(02)	LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-06(02)_ODP	***security functions or security-relevant information, the access to which requires users to use non-privileged accounts to access non-security functions, are defined;***
	AC-06(02)	users of system accounts (or roles) with access to ***<AC-06(02)_ODP security functions or security-relevant information>*** are required to use non-privileged accounts or roles when accessing non-security functions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-06(02)-Examine	[SELECT FROM: Access control policy; procedures addressing least privilege; list of system-generated security functions or security-relevant information assigned to system accounts or roles; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-06(02)-Interview	[SELECT FROM: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators].
	AC-06(02)-Test	[SELECT FROM: Mechanisms implementing least privilege functions].

AC-06(03)	LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-06(03)_ODP[01]	***privileged commands to which network access is to be authorized only for compelling operational needs are defined;***
	AC-06(03)_ODP[02]	***compelling operational needs necessitating network access to privileged commands are defined;***
	AC-06(03)[01]	network access to ***<AC-06(03)_ODP[01] privileged commands>*** is authorized only for ***<AC-06(03)_ODP[02] compelling operational needs>***;
	AC-06(03)[02]	the rationale for authorizing network access to privileged commands is documented in the security plan for the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-06(03)-Examine	[SELECT FROM: Access control policy; procedures addressing least privilege; system configuration settings and associated documentation; system audit records; list of operational needs for authorizing network access to privileged commands; system security plan; other relevant documents or records].
	AC-06(03)-Interview	[SELECT FROM: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities].
	AC-06(03)-Test	[SELECT FROM: Mechanisms implementing least privilege functions].

AC-06(04)	LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-06(04)	separate processing domains are provided to enable finer-grain allocation of user privileges.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-06(04)-Examine	[SELECT FROM: Access control policy; procedures addressing least privilege; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-06(04)-Interview	[SELECT FROM: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system developers].
	AC-06(04)-Test	[SELECT FROM: Mechanisms implementing least privilege functions].

AC-06(05)	LEAST PRIVILEGE | PRIVILEGED ACCOUNTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-06(05)_ODP	***personnel or roles to which privileged accounts on the system are to be restricted is/are defined;***
	AC-06(05)	privileged accounts on the system are restricted to ***<AC-06(05)_ODP personnel or roles>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-06(05)-Examine	[SELECT FROM: Access control policy; procedures addressing least privilege; list of system-generated privileged accounts; list of system administration personnel; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-06(05)-Interview	[SELECT FROM: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators].
	AC-06(05)-Test	[SELECT FROM: Mechanisms implementing least privilege functions].

AC-06(06)	LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-06(06)	privileged access to the system by non-organizational users is prohibited.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-06(06)-Examine	[SELECT FROM: Access control policy; procedures addressing least privilege; list of system-generated privileged accounts; list of non-organizational users; system configuration settings and associated documentation; audit records; system security plan; other relevant documents or records].
	AC-06(06)-Interview	[SELECT FROM: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators].
	AC-06(06)-Test	[SELECT FROM: Mechanisms prohibiting privileged access to the system].

AC-06(07)	LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-06(07)_ODP[01]	***the frequency at which to review the privileges assigned to roles or classes of users is defined;***
	AC-06(07)_ODP[02]	***roles or classes of users to which privileges are assigned are defined;***
	AC-06(07)(a)	privileges assigned to ***<AC-06(07)_ODP[02] roles and classes>*** are reviewed ***<AC-06(07)_ODP[01] frequency>*** to validate the need for such privileges;

AC-06(07)	LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES	
	AC-06(07)(b)	privileges are reassigned or removed, if necessary, to correctly reflect organizational mission and business needs.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-06(07)-Examine	[SELECT FROM: Access control policy; procedures addressing least privilege; list of system-generated roles or classes of users and assigned privileges; system design documentation; system configuration settings and associated documentation; validation reviews of privileges assigned to roles or classes or users; records of privilege removals or reassignments for roles or classes of users; system audit records; system security plan; other relevant documents or records].
	AC-06(07)-Interview	[SELECT FROM: Organizational personnel with responsibilities for reviewing least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators].
	AC-06(07)-Test	[SELECT FROM: Mechanisms implementing review of user privileges].

AC-06(08)	LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-06(08)_ODP	***software to be prevented from executing at higher privilege levels than users executing the software is defined;***
	AC-06(08)	***<AC-06(08)_ODP software>*** is prevented from executing at higher privilege levels than users executing the software.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-06(08)-Examine	[SELECT FROM: Access control policy; procedures addressing least privilege; list of software that should not execute at higher privilege levels than users executing software; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-06(08)-Interview	[SELECT FROM: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators; system developers].
	AC-06(08)-Test	[SELECT FROM: Mechanisms implementing least privilege functions for software execution].

AC-06(09)	LEAST PRIVILEGE | LOG USE OF PRIVILEGED FUNCTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-06(09)	the execution of privileged functions is logged.

AC-06(09)	LEAST PRIVILEGE | LOG USE OF PRIVILEGED FUNCTIONS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-06(09)-Examine	[SELECT FROM: Access control policy; procedures addressing least privilege; system design documentation; system configuration settings and associated documentation; list of privileged functions to be audited; list of audited events; system audit records; system security plan; other relevant documents or records].
	AC-06(09)-Interview	[SELECT FROM: Organizational personnel with responsibilities for reviewing least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators; system developers].
	AC-06(09)-Test	[SELECT FROM: Mechanisms auditing the execution of least privilege functions].

AC-06(10)	LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-06(10)	non-privileged users are prevented from executing privileged functions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-06(10)-Examine	[SELECT FROM: Access control policy; procedures addressing least privilege; system design documentation; system configuration settings and associated documentation; list of privileged functions and associated user account assignments; system audit records; system security plan; other relevant documents or records].
	AC-06(10)-Interview	[SELECT FROM: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system developers].
	AC-06(10)-Test	[SELECT FROM: Mechanisms implementing least privilege functions for non-privileged users].

AC-07	UNSUCCESSFUL LOGON ATTEMPTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-07_ODP[01]	***the number of consecutive invalid logon attempts by a user allowed during a time period is defined;***
	AC-07_ODP[02]	***the time period to which the number of consecutive invalid logon attempts by a user is limited is defined;***
	AC-07_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {lock the account or node for <AC-07_ODP[04] time period>; lock the account or node until released by an administrator; delay next logon prompt per <AC-07_ODP[05] delay algorithm>; notify system administrator; take other <AC-07_ODP[06] action>};***
	AC-07_ODP[04]	***time period for an account or node to be locked is defined (if selected);***

AC-07	UNSUCCESSFUL LOGON ATTEMPTS	
	AC-07_ODP[05]	***delay algorithm for the next logon prompt is defined (if selected);***
	AC-07_ODP[06]	***other action to be taken when the maximum number of unsuccessful attempts is exceeded is defined (if selected);***
	AC-07a.	a limit of ***<AC-07_ODP[01] number>*** consecutive invalid logon attempts by a user during ***<AC-07_ODP[02] time period>*** is enforced;
	AC-07b.	automatically ***<AC-07_ODP[03] SELECTED PARAMETER VALUE(S)>*** when the maximum number of unsuccessful attempts is exceeded.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-07-Examine	[SELECT FROM: Access control policy; procedures addressing unsuccessful logon attempts; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-07-Interview	[SELECT FROM: Organizational personnel with information security responsibilities; system developers; system/network administrators].
	AC-07-Test	[SELECT FROM: Mechanisms implementing access control policy for unsuccessful logon attempts].

AC-07(01)	UNSUCCESSFUL LOGON ATTEMPTS | AUTOMATIC ACCOUNT LOCK
	[WITHDRAWN: Incorporated into AC-07.]

AC-07(02)	UNSUCCESSFUL LOGON ATTEMPTS | PURGE OR WIPE MOBILE DEVICE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-07(02)_ODP[01]	***mobile devices to be purged or wiped of information are defined;***
	AC-07(02)_ODP[02]	***purging or wiping requirements and techniques to be used when mobile devices are purged or wiped of information are defined;***
	AC-07(02)_ODP[03]	***the number of consecutive, unsuccessful logon attempts before the information is purged or wiped from mobile devices is defined;***
	AC-07(02)	information is purged or wiped from ***<AC-07(02)_ODP[01] mobile devices>*** based on ***<AC-07(02)_ODP[02] purging or wiping requirements or techniques>*** after ***<AC-07(02)_ODP[03] number>*** consecutive, unsuccessful device logon attempts.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-07(02)-Examine	[SELECT FROM: Access control policy; procedures addressing unsuccessful logon attempts on mobile devices; system design documentation; system configuration settings and associated documentation; list of mobile devices to be purged/wiped after organization-defined consecutive, unsuccessful device logon attempts; list of purging/wiping requirements or techniques for mobile devices; system audit records; system security plan; other relevant documents or records].

AC-07(02)	UNSUCCESSFUL LOGON ATTEMPTS | PURGE OR WIPE MOBILE DEVICE	
	AC-07(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	AC-07(02)-Test	[SELECT FROM: Mechanisms implementing access control policy for unsuccessful device logon attempts].

AC-07(03)	UNSUCCESSFUL LOGON ATTEMPTS | BIOMETRIC ATTEMPT LIMITING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-07(03)_ODP	***the number of unsuccessful biometric logon attempts is defined;***
	AC-07(03)	unsuccessful biometric logon attempts are limited to ***<AC-07(03)_ODP number>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-07(03)-Examine	[SELECT FROM: Access control policy; procedures addressing unsuccessful logon attempts on biometric devices; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-07(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	AC-07(03)-Test	[SELECT FROM: Mechanisms implementing access control policy for unsuccessful logon attempts].

AC-07(04)	UNSUCCESSFUL LOGON ATTEMPTS | USE OF ALTERNATE AUTHENTICATION FACTOR	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-07(04)_ODP[01]	***authentication factors allowed to be used that are different from the primary authentication factors are defined;***
	AC-07(04)_ODP[02]	***the number of consecutive, invalid logon attempts through the use of alternative factors for which to enforce a limit by a user is defined;***
	AC-07(04)_ODP[03]	***time period during which a user can attempt logons through alternative factors is defined;***
	AC-07(04)(a)	***<AC-07(04)_ODP[01] authentication factors>*** that are different from the primary authentication factors are allowed to be used after the number of organization-defined consecutive invalid logon attempts have been exceeded;
	AC-07(04)(b)	a limit of ***<AC-07(04)_ODP[02] number>*** consecutive invalid logon attempts through the use of the alternative factors by the user during a ***<AC-07(04)_ODP[03] time period>*** is enforced.

AC-07(04)	UNSUCCESSFUL LOGON ATTEMPTS | USE OF ALTERNATE AUTHENTICATION FACTOR	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-07(04)-Examine	[SELECT FROM: Access control policy; procedures addressing unsuccessful logon attempts for primary and alternate authentication factors; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-07(04)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	AC-07(04)-Test	[SELECT FROM: Mechanisms implementing access control policy for unsuccessful logon attempts].

AC-08	SYSTEM USE NOTIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-08_ODP[01]	***system use notification message or banner to be displayed by the system to users before granting access to the system is defined;***
	AC-08_ODP[02]	***conditions for system use to be displayed by the system before granting further access are defined;***
	AC-08a.	***<AC-08_ODP[01] system use notification>*** is displayed to users before granting access to the system that provides privacy and security notices consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines;
	AC-08a.01	the system use notification states that users are accessing a U.S. Government system;
	AC-08a.02	the system use notification states that system usage may be monitored, recorded, and subject to audit;
	AC-08a.03	the system use notification states that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
	AC-08a.04	the system use notification states that use of the system indicates consent to monitoring and recording;
	AC-08b.	the notification message or banner is retained on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system;
	AC-08c.01	for publicly accessible systems, system use information ***<AC-08_ODP[02] conditions>*** is displayed before granting further access to the publicly accessible system;
	AC-08c.02	for publicly accessible systems, any references to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities are displayed;
	AC-08c.03	for publicly accessible systems, a description of the authorized uses of the system is included.

AC-08	SYSTEM USE NOTIFICATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-08-Examine	[SELECT FROM: Access control policy; privacy and security policies, procedures addressing system use notification; documented approval of system use notification messages or banners; system audit records; user acknowledgements of notification message or banner; system design documentation; system configuration settings and associated documentation; system use notification messages; system security plan; privacy plan; privacy impact assessment; privacy assessment report; other relevant documents or records].
	AC-08-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; legal counsel; system developers].
	AC-08-Test	[SELECT FROM: Mechanisms implementing system use notification].

AC-09	PREVIOUS LOGON NOTIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-09	the user is notified, upon successful logon to the system, of the date and time of the last logon.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-09-Examine	[SELECT FROM: Access control policy; procedures addressing previous logon notification; system design documentation; system configuration settings and associated documentation; system notification messages; system security plan; other relevant documents or records].
	AC-09-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-09-Test	[SELECT FROM: Mechanisms implementing access control policy for previous logon notification].

AC-09(01)	PREVIOUS LOGON NOTIFICATION | UNSUCCESSFUL LOGONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-09(01)	the user is notified, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-09(01)-Examine	[SELECT FROM: Access control policy; procedures addressing previous logon notification; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-09(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].

AC-09(01)	PREVIOUS LOGON NOTIFICATION | UNSUCCESSFUL LOGONS	
	AC-09(01)-Test	[SELECT FROM: Mechanisms implementing access control policy for previous logon notification].

AC-09(02)	PREVIOUS LOGON NOTIFICATION | SUCCESSFUL AND UNSUCCESSFUL LOGONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-09(02)_ODP[01]	***one of the following PARAMETER VALUES is selected: {successful logons; unsuccessful logon attempts; both};***
	AC-09(02)_ODP[02]	***the time period for which the system notifies the user of the number of successful logons, unsuccessful logon attempts, or both is defined;***
	AC-09(02)	the user is notified, upon successful logon, of the number of ***<AC-09(02)_ODP[01] SELECTED PARAMETER VALUE>*** during ***<AC-09(02)_ODP[02] time period>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-09(02)-Examine	[SELECT FROM: Access control policy; procedures addressing previous logon notification; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-09(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-09(02)-Test	[SELECT FROM: Mechanisms implementing access control policy for previous logon notification].

AC-09(03)	PREVIOUS LOGON NOTIFICATION | NOTIFICATION OF ACCOUNT CHANGES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-09(03)_ODP[01]	***changes to security-related characteristics or parameters of the user's account that require notification are defined;***
	AC-09(03)_ODP[02]	***the time period for which the system notifies the user of changes to security-related characteristics or parameters of the user's account is defined;***
	AC-09(03)	the user is notified, upon successful logon, of changes to ***<AC-09(03)_ODP[01] security-related characteristics or parameters>*** during ***<AC-09(03)_ODP[02] time period>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-09(03)-Examine	[SELECT FROM: Access control policy; procedures addressing previous logon notification; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-09(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].

AC-09(03)	PREVIOUS LOGON NOTIFICATION | NOTIFICATION OF ACCOUNT CHANGES	
	AC-09(03)-Test	[SELECT FROM: Mechanisms implementing access control policy for previous logon notification].

AC-09(04)	PREVIOUS LOGON NOTIFICATION | ADDITIONAL LOGON INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-09(04)_ODP	***additional information about which to notify the user is defined;***
	AC-09(04)	the user is notified, upon successful logon, of ***<AC-09(04)_ODP additional information>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-09(04)-Examine	[SELECT FROM: Access control policy; procedures addressing previous logon notification; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-09(04)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-09(04)-Test	[SELECT FROM: Mechanisms implementing access control policy for previous logon notification].

AC-10	CONCURRENT SESSION CONTROL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-10_ODP[01]	***accounts and/or account types for which to limit the number of concurrent sessions is defined;***
	AC-10_ODP[02]	***the number of concurrent sessions to be allowed for each account and/or account type is defined;***
	AC-10	the number of concurrent sessions for each ***<AC-10_ODP[01] account and/or account types>*** is limited to ***<AC-10_ODP[02] number>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-10-Examine	[SELECT FROM: Access control policy; procedures addressing concurrent session control; system design documentation; system configuration settings and associated documentation; security plan; system security plan; other relevant documents or records].
	AC-10-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-10-Test	[SELECT FROM: Mechanisms implementing access control policy for concurrent session control].

AC-11	DEVICE LOCK	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-11_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {initiating a device lock after <AC-11_ODP[02] time period> of inactivity; requiring the user to initiate a device lock before leaving the system unattended};***
	AC-11_ODP[02]	***time period of inactivity after which a device lock is initiated is defined (if selected);***
	AC-11a.	further access to the system is prevented by ***<AC-11_ODP[01] SELECTED PARAMETER VALUE(S)>***;
	AC-11b.	device lock is retained until the user re-establishes access using established identification and authentication procedures.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-11-Examine	[SELECT FROM: Access control policy; procedures addressing session lock; procedures addressing identification and authentication; system design documentation; system configuration settings and associated documentation; security plan; system security plan; other relevant documents or records].
	AC-11-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-11-Test	[SELECT FROM: Mechanisms implementing access control policy for session lock].

AC-11(01)	DEVICE LOCK | PATTERN-HIDING DISPLAYS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-11(01)	information previously visible on the display is concealed, via device lock, with a publicly viewable image.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-11(01)-Examine	[SELECT FROM: Access control policy; procedures addressing session lock; display screen with session lock activated; system design documentation; system configuration settings and associated documentation; system security plan; other relevant documents or records].
	AC-11(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-11(01)-Test	[SELECT FROM: System session lock mechanisms].

AC-12	SESSION TERMINATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-12_ODP	***conditions or trigger events requiring session disconnect are defined;***

AC-12	SESSION TERMINATION	
	AC-12	a user session is automatically terminated after ***<AC-12_ODP conditions or trigger events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-12-Examine	[SELECT FROM: Access control policy; procedures addressing session termination; system design documentation; system configuration settings and associated documentation; list of conditions or trigger events requiring session disconnect; system audit records; system security plan; other relevant documents or records].
	AC-12-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-12-Test	[SELECT FROM: Automated mechanisms implementing user session termination].

AC-12(01)	SESSION TERMINATION | USER-INITIATED LOGOUTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-12(01)_ODP	***information resources for which a logout capability for user-initiated communications sessions is required are defined;***
	AC-12(01)	a logout capability is provided for user-initiated communications sessions whenever authentication is used to gain access to ***<AC-12(01)_ODP information resources>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-12(01)-Examine	[SELECT FROM: Access control policy; procedures addressing session termination; user logout messages; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-12(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-12(01)-Test	[SELECT FROM: System session termination mechanisms; logout capabilities for user-initiated communications sessions].

AC-12(02)	SESSION TERMINATION | TERMINATION MESSAGE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-12(02)	an explicit logout message is displayed to users indicating the termination of authenticated communication sessions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-12(02)-Examine	[SELECT FROM: Access control policy; procedures addressing session termination; user logout messages; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].

AC-12(02)	SESSION TERMINATION | TERMINATION MESSAGE	
	AC-12(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-12(02)-Test	[SELECT FROM: System session termination mechanisms; display of logout messages].

AC-12(03)	SESSION TERMINATION | TIMEOUT WARNING MESSAGE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-12(03)_ODP	***time until the end of session for display to users is defined;***
	AC-12(03)	an explicit message to users is displayed indicating that the session will end in ***<AC-12(03)_ODP time>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-12(03)-Examine	[SELECT FROM: Access control policy; procedures addressing session termination; time until end of session messages; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-12(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-12(03)-Test	[SELECT FROM: System session termination mechanisms; display of end of session time].

AC-13	SUPERVISION AND REVIEW — ACCESS CONTROL	
	[WITHDRAWN: Incorporated into AC-02, AU-06.]	

AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-14_ODP	***user actions that can be performed on the system without identification or authentication are defined;***
	AC-14a.	***<AC-14_ODP user actions>*** that can be performed on the system without identification or authentication consistent with organizational mission and business functions are identified;
	AC-14b.[01]	user actions not requiring identification or authentication are documented in the security plan for the system;
	AC-14b.[02]	a rationale for user actions not requiring identification or authentication is provided in the security plan for the system.

AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-14-Examine	[SELECT FROM: Access control policy; procedures addressing permitted actions without identification or authentication; system configuration settings and associated documentation; security plan; list of user actions that can be performed without identification or authentication; system audit records; system security plan; other relevant documents or records].
	AC-14-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].

AC-14(01)	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION | NECESSARY USES
	[WITHDRAWN: Incorporated into AC-14.]

AC-15	AUTOMATED MARKING
	[WITHDRAWN: Incorporated into MP-03.]

AC-16	SECURITY AND PRIVACY ATTRIBUTES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-16_ODP[01]	***types of security attributes to be associated with information security attribute values for information in storage, in process, and/or in transmission are defined;***
	AC-16_ODP[02]	***types of privacy attributes to be associated with privacy attribute values for information in storage, in process, and/or in transmission are defined;***
	AC-16_ODP[03]	***security attribute values for types of security attributes are defined;***
	AC-16_ODP[04]	***privacy attribute values for types of privacy attributes are defined;***
	AC-16_ODP[05]	***systems for which permitted security attributes are to be established are defined;***
	AC-16_ODP[06]	***systems for which permitted privacy attributes are to be established are defined;***
	AC-16_ODP[07]	***security attributes defined as part of AC-16a that are permitted for systems are defined;***
	AC-16_ODP[08]	***privacy attributes defined as part of AC-16a that are permitted for systems are defined;***
	AC-16_ODP[09]	***attribute values or ranges for established attributes are defined;***
	AC-16_ODP[10]	***the frequency at which to review security attributes for applicability is defined;***
	AC-16_ODP[11]	***the frequency at which to review privacy attributes for applicability is defined;***

AC-16	SECURITY AND PRIVACY ATTRIBUTES	
	AC-16a.[01]	the means to associate ***<AC-16_ODP[01] types of security attributes>*** with ***<AC-16_ODP[03] security attribute values>*** for information in storage, in process, and/or in transmission are provided;
	AC-16a.[02]	the means to associate ***<AC-16_ODP[02] types of privacy attributes>*** with ***<AC-16_ODP[04] privacy attribute values>*** for information in storage, in process, and/or in transmission are provided;
	AC-16b.[01]	attribute associations are made;
	AC-16b.[02]	attribute associations are retained with the information;
	AC-16c.[01]	the following permitted security attributes are established from the attributes defined in AC-16_ODP[01] for ***<AC-16_ODP[05] systems>***: ***<AC-16_ODP[07] security attributes>***;
	AC-16c.[02]	the following permitted privacy attributes are established from the attributes defined in AC-16_ODP[02] for ***<AC-16_ODP[06] systems>***: ***<AC-16_ODP[08] privacy attributes>***;
	AC-16d.	the following permitted attribute values or ranges for each of the established attributes are determined: ***<AC-16_ODP[09] attribute values or ranges>***;
	AC-16e.	changes to attributes are audited;
	AC-16f.[01]	***<AC-16_ODP[07] security attributes>*** are reviewed for applicability ***<AC-16_ODP[10] frequency>***;
	AC-16f.[02]	***<AC-16_ODP[08] privacy attributes>*** are reviewed for applicability ***<AC-16_ODP[11] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-16-Examine	[SELECT FROM: Access control policy; procedures addressing the association of security and privacy attributes to information in storage, in process, and in transmission; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-16-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; system developers].
	AC-16-Test	[SELECT FROM: Organizational capability supporting and maintaining the association of security and privacy attributes to information in storage, in process, and in transmission].

AC-16(01)	SECURITY AND PRIVACY ATTRIBUTES | DYNAMIC ATTRIBUTE ASSOCIATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-16(01)_ODP[01]	***subjects with which security attributes are to be dynamically associated as information is created and combined are defined;***
	AC-16(01)_ODP[02]	***objects with which security attributes are to be dynamically associated as information is created and combined are defined;***

AC-16(01)	SECURITY AND PRIVACY ATTRIBUTES | DYNAMIC ATTRIBUTE ASSOCIATION	
	AC-16(01)_ODP[03]	***subjects with which privacy attributes are to be dynamically associated as information is created and combined are defined;***
	AC-16(01)_ODP[04]	***objects with which privacy attributes are to be dynamically associated as information is created and combined are defined;***
	AC-16(01)_ODP[05]	***security policies requiring dynamic association of security attributes with subjects and objects are defined;***
	AC-16(01)_ODP[06]	***privacy policies requiring dynamic association of privacy attributes with subjects and objects are defined;***
	AC-16(01)[01]	security attributes are dynamically associated with ***<AC-16(01)_ODP[01] subjects>*** in accordance with the following security policies as information is created and combined: ***<AC-16(01)_ODP[05] security policies>***;
	AC-16(01)[02]	security attributes are dynamically associated with ***<AC-16(01)_ODP[02] objects>*** in accordance with the following security policies as information is created and combined: ***<AC-16(01)_ODP[05] security policies>***;
	AC-16(01)[03]	privacy attributes are dynamically associated with ***<AC-16(01)_ODP[03] subjects>*** in accordance with the following privacy policies as information is created and combined: ***<AC-16(01)_ODP[06] privacy policies>***;
	AC-16(01)[04]	privacy attributes are dynamically associated with ***<AC-16(01)_ODP[04] objects>*** in accordance with the following privacy policies as information is created and combined: ***<AC-16(01)_ODP[06] privacy policies>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-16(01)-Examine	[SELECT FROM: Access control policy; procedures addressing dynamic association of security and privacy attributes to information; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-16(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; system developers].
	AC-16(01)-Test	[SELECT FROM: Automated mechanisms implementing dynamic association of security and privacy attributes to information].

AC-16(02)	SECURITY AND PRIVACY ATTRIBUTES | ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-16(02)[01]	authorized individuals (or processes acting on behalf of individuals) are provided with the capability to define or change the value of associated security attributes;
	AC-16(02)[02]	authorized individuals (or processes acting on behalf of individuals) are provided with the capability to define or change the value of associated privacy attributes.

AC-16(02)	SECURITY AND PRIVACY ATTRIBUTES | ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-16(02)-Examine	[SELECT FROM: Access control policy; procedures addressing the change of security and privacy attribute values; system design documentation; system configuration settings and associated documentation; list of individuals authorized to change security and privacy attributes; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-16(02)-Interview	[SELECT FROM: Organizational personnel with responsibilities for changing values of security and privacy attributes; organizational personnel with information security and privacy responsibilities; system developers].
	AC-16(02)-Test	[SELECT FROM: Mechanisms permitting changes to values of security and privacy attributes].

AC-16(03)	SECURITY AND PRIVACY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY SYSTEM	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-16(03)_ODP[01]	***security attributes that require association and integrity maintenance are defined;***
	AC-16(03)_ODP[02]	***privacy attributes that require association and integrity maintenance are defined;***
	AC-16(03)_ODP[03]	***subjects requiring the association and integrity of security attributes to such subjects to be maintained are defined;***
	AC-16(03)_ODP[04]	***objects requiring the association and integrity of security attributes to such objects to be maintained are defined;***
	AC-16(03)_ODP[05]	***subjects requiring the association and integrity of privacy attributes to such subjects to be maintained are defined;***
	AC-16(03)_ODP[06]	***objects requiring the association and integrity of privacy attributes to such objects to be maintained are defined;***
	AC-16(03)[01]	the association and integrity of ***<AC-16(03)_ODP[01] security attributes>*** to ***<AC-16(03)_ODP[03] subjects>*** is maintained;
	AC-16(03)[02]	the association and integrity of ***<AC-16(03)_ODP[01] security attributes>*** to ***<AC-16(03)_ODP[04] objects>*** is maintained.
	AC-16(03)[03]	the association and integrity of ***<AC-16(03)_ODP[02] privacy attributes>*** to ***<AC-16(03)_ODP[05] subjects>*** is maintained;
	AC-16(03)[04]	the association and integrity of ***<AC-16(03)_ODP[02] privacy attributes>*** to ***<AC-16(03)_ODP[06] objects>*** is maintained.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-16(03)-Examine	[SELECT FROM: Access control policy; procedures addressing the association of security and privacy attributes to information; procedures addressing labeling or marking; system design documentation; system configuration settings and associated documentation; system security plan; privacy plan; other relevant documents or records].

AC-16(03)	SECURITY AND PRIVACY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY SYSTEM	
	AC-16(03)-Interview	[SELECT FROM: Organizational personnel with information security and privacy responsibilities; system developers].
	AC-16(03)-Test	[SELECT FROM: Mechanisms maintaining association and integrity of security and privacy attributes to information].

AC-16(04)	SECURITY AND PRIVACY ATTRIBUTES | ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-16(04)_ODP[01]	***security attributes to be associated with subjects by authorized individuals (or processes acting on behalf of individuals) are defined;***
	AC-16(04)_ODP[02]	***security attributes to be associated with objects by authorized individuals (or processes acting on behalf of individuals) are defined;***
	AC-16(04)_ODP[03]	***privacy attributes to be associated with subjects by authorized individuals (or processes acting on behalf of individuals) are defined;***
	AC-16(04)_ODP[04]	***privacy attributes to be associated with objects by authorized individuals (or processes acting on behalf of individuals) are defined;***
	AC-16(04)_ODP[05]	***subjects requiring the association of security attributes by authorized individuals (or processes acting on behalf of individuals) are defined;***
	AC-16(04)_ODP[06]	***objects requiring the association of security attributes by authorized individuals (or processes acting on behalf of individuals) are defined;***
	AC-16(04)_ODP[07]	***subjects requiring the association of privacy attributes by authorized individuals (or processes acting on behalf of individuals) are defined;***
	AC-16(04)_ODP[08]	***objects requiring the association of privacy attributes by authorized individuals (or processes acting on behalf of individuals) are defined;***
	AC-16(04)[01]	authorized individuals (or processes acting on behalf of individuals) are provided with the capability to associate ***<AC-16(04)_ODP[01] security attributes>*** with ***<AC-16(04)_ODP[05] subjects>***;
	AC-16(04)[02]	authorized individuals (or processes acting on behalf of individuals) are provided with the capability to associate ***<AC-16(04)_ODP[02] security attributes>*** with ***<AC-16(04)_ODP[06] objects>***;
	AC-16(04)[03]	authorized individuals (or processes acting on behalf of individuals) are provided with the capability to associate ***<AC-16(04)_ODP[03] privacy attributes>*** with ***<AC-16(04)_ODP[07] subjects>***;
	AC-16(04)[04]	authorized individuals (or processes acting on behalf of individuals) are provided with the capability to associate ***<AC-16(04)_ODP[04] privacy attributes>*** with ***<AC-16(04)_ODP[08] objects>***.

AC-16(04)	SECURITY AND PRIVACY ATTRIBUTES | ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-16(04)-Examine	[SELECT FROM: Access control policy; procedures addressing the association of security and privacy attributes to information; system design documentation; system configuration settings and associated documentation; list of users authorized to associate security and privacy attributes to information; system prompts for privileged users to select security and privacy attributes to be associated with information objects; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-16(04)-Interview	[SELECT FROM: Organizational personnel with responsibilities for associating security and privacy attributes to information; organizational personnel with information security and privacy responsibilities; system developers].
	AC-16(04)-Test	[SELECT FROM: Mechanisms supporting user associations of security and privacy attributes to information].

AC-16(05)	SECURITY AND PRIVACY ATTRIBUTES | ATTRIBUTE DISPLAYS ON OBJECTS TO BE OUTPUT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-16(05)_ODP[01]	***special dissemination, handling, or distribution instructions to be used for each object that the system transmits to output devices are defined;***
	AC-16(05)_ODP[02]	***human-readable, standard naming conventions for the security and privacy attributes to be displayed in human-readable form on each object that the system transmits to output devices are defined;***
	AC-16(05)[01]	security attributes are displayed in human-readable form on each object that the system transmits to output devices to identify ***<AC-16(05)_ODP[01] instructions>*** using ***<AC-16(05)_ODP[02] naming conventions>***;
	AC-16(05)[02]	privacy attributes are displayed in human-readable form on each object that the system transmits to output devices to identify ***<AC-16(05)_ODP[01] instructions>*** using ***<AC-16(05)_ODP[02] naming conventions>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-16(05)-Examine	[SELECT FROM: Access control policy; procedures addressing display of security and privacy attributes in human-readable form; special dissemination, handling, or distribution instructions; types of human-readable, standard naming conventions; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-16(05)-Interview	[SELECT FROM: Organizational personnel with information security and privacy responsibilities; system developers].
	AC-16(05)-Test	[SELECT FROM: System output devices displaying security and privacy attributes in human-readable form on each object].

AC-16(06)	SECURITY AND PRIVACY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-16(06)_ODP[01]	***security attributes to be associated with subjects are defined;***
	AC-16(06)_ODP[02]	***security attributes to be associated with objects are defined;***
	AC-16(06)_ODP[03]	***privacy attributes to be associated with subjects are defined;***
	AC-16(06)_ODP[04]	***privacy attributes to be associated with objects are defined;***
	AC-16(06)_ODP[05]	***subjects to be associated with information security attributes are defined;***
	AC-16(06)_ODP[06]	***objects to be associated with information security attributes are defined;***
	AC-16(06)_ODP[07]	***subjects to be associated with privacy attributes are defined;***
	AC-16(06)_ODP[08]	***objects to be associated with privacy attributes are defined;***
	AC-16(06)_ODP[09]	***security policies that require personnel to associate and maintain the association of security and privacy attributes with subjects and objects;***
	AC-16(06)_ODP[10]	***privacy policies that require personnel to associate and maintain the association of security and privacy attributes with subjects and objects;***
	AC-16(06)[01]	personnel are required to associate and maintain the association of ***<AC-16(06)_ODP[01] security attributes>*** with ***<AC-16(06)_ODP[05] subjects>*** in accordance with ***<AC-16(06)_ODP[09] security policies>***;
	AC-16(06)[02]	personnel are required to associate and maintain the association of ***<AC-16(06)_ODP[02] security attributes>*** with ***<AC-16(06)_ODP[06] objects>*** in accordance with ***<AC-16(06)_ODP[09] security policies>***;
	AC-16(06)[03]	personnel are required to associate and maintain the association of ***<AC-16(06)_ODP[03] privacy attributes>*** with ***<AC-16(06)_ODP[07] subjects>*** in accordance with ***<AC-16(06)_ODP[10] privacy policies>***;
	AC-16(06)[04]	personnel are required to associate and maintain the association of ***<AC-16(06)_ODP[04] privacy attributes>*** with ***<AC-16(06)_ODP[08] objects>*** in accordance with ***<AC-16(06)_ODP[10] privacy policies>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-16(06)-Examine	[SELECT FROM: Access control policy; procedures addressing association of security and privacy attributes with subjects and objects; system security plan; privacy plan; other relevant documents or records].
	AC-16(06)-Interview	[SELECT FROM: Organizational personnel with responsibilities for associating and maintaining association of security and privacy attributes with subjects and objects; organizational personnel with information security and privacy responsibilities; system developers].
	AC-16(06)-Test	[SELECT FROM: Mechanisms supporting associations of security and privacy attributes to subjects and objects].

AC-16(07)	SECURITY AND PRIVACY ATTRIBUTES | CONSISTENT ATTRIBUTE INTERPRETATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-16(07)[01]	a consistent interpretation of security attributes transmitted between distributed system components is provided;
	AC-16(07)[02]	a consistent interpretation of privacy attributes transmitted between distributed system components is provided.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-16(07)-Examine	[SELECT FROM: Access control policies and procedures; procedures addressing consistent interpretation of security and privacy attributes transmitted between distributed system components; procedures addressing access enforcement; procedures addressing information flow enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy access control policy; other relevant documents or records].
	AC-16(07)-Interview	[SELECT FROM: Organizational personnel with responsibilities for providing consistent interpretation of security and privacy attributes used in access enforcement and information flow enforcement actions; organizational personnel with information security and privacy responsibilities; system developers].
	AC-16(07)-Test	[SELECT FROM: Mechanisms implementing access enforcement and information flow enforcement functions].

AC-16(08)	SECURITY AND PRIVACY ATTRIBUTES | ASSOCIATION TECHNIQUES AND TECHNOLOGIES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-16(08)_ODP[01]	***techniques and technologies to be implemented in associating security attributes to information are defined;***
	AC-16(08)_ODP[02]	***techniques and technologies to be implemented in associating privacy attributes to information are defined;***
	AC-16(08)[01]	***<AC-16(08)_ODP[01] techniques and technologies>*** are implemented in associating security attributes to information;
	AC-16(08)[02]	***<AC-16(08)_ODP[02] techniques and technologies>*** are implemented in associating privacy attributes to information.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-16(08)-Examine	[SELECT FROM: Access control policy; procedures addressing association of security and privacy attributes to information; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-16(08)-Interview	[SELECT FROM: Organizational personnel with responsibilities for associating security and privacy attributes to information; organizational personnel with information security and privacy responsibilities; system developers].
	AC-16(08)-Test	[SELECT FROM: Mechanisms implementing techniques or technologies associating security and privacy attributes to information].

AC-16(09)	SECURITY AND PRIVACY ATTRIBUTES | ATTRIBUTE REASSIGNMENT — REGRADING MECHANISMS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-16(09)_ODP[01]	***techniques or procedures used to validate regrading mechanisms for security attributes are defined;***
	AC-16(09)_ODP[02]	***techniques or procedures used to validate regrading mechanisms for privacy attributes are defined;***
	AC-16(09)[01]	security attributes associated with information are changed only via regrading mechanisms validated using ***<AC-16(09)_ODP[01] techniques or procedures>***;
	AC-16(09)[02]	privacy attributes associated with information are changed only via regrading mechanisms validated using ***<AC-16(09)_ODP[02] techniques or procedures>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-16(09)-Examine	[SELECT FROM: Access control policy; procedures addressing reassignment of security attributes to information; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-16(09)-Interview	[SELECT FROM: Organizational personnel with responsibilities for reassigning association of security and privacy attributes to information; organizational personnel with information security and privacy responsibilities; system developers].
	AC-16(09)-Test	[SELECT FROM: Mechanisms implementing techniques or procedures for reassigning association of security and privacy attributes to information].

AC-16(10)	SECURITY AND PRIVACY ATTRIBUTES | ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-16(10)[01]	authorized individuals are provided with the capability to define or change the type and value of security attributes available for association with subjects and objects;
	AC-16(10)[02]	authorized individuals are provided with the capability to define or change the type and value of privacy attributes available for association with subjects and objects.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-16(10)-Examine	[SELECT FROM: Access control policy; procedures addressing configuration of security and privacy attributes by authorized individuals; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-16(10)-Interview	[SELECT FROM: Organizational personnel with responsibilities for defining or changing security and privacy attributes associated with information; organizational personnel with information security and privacy responsibilities; system developers].

AC-16(10)	SECURITY AND PRIVACY ATTRIBUTES | ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS	
	AC-16(10)-Test	[SELECT FROM: Mechanisms implementing capability for defining or changing security and privacy attributes].

AC-17	REMOTE ACCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-17a.[01]	usage restrictions are established and documented for each type of remote access allowed;
	AC-17a.[02]	configuration/connection requirements are established and documented for each type of remote access allowed;
	AC-17a.[03]	implementation guidance is established and documented for each type of remote access allowed;
	AC-17b.	each type of remote access to the system is authorized prior to allowing such connections.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-17-Examine	[SELECT FROM: Access control policy; procedures addressing remote access implementation and usage (including restrictions); configuration management plan; system configuration settings and associated documentation; remote access authorizations; system audit records; system security plan; other relevant documents or records].
	AC-17-Interview	[SELECT FROM: Organizational personnel with responsibilities for managing remote access connections; system/network administrators; organizational personnel with information security responsibilities].
	AC-17-Test	[SELECT FROM: Remote access management capability for the system].

AC-17(01)	REMOTE ACCESS | MONITORING AND CONTROL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-17(01)[01]	automated mechanisms are employed to monitor remote access methods;
	AC-17(01)[02]	automated mechanisms are employed to control remote access methods.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-17(01)-Examine	[SELECT FROM: Access control policy; procedures addressing remote access to the system; system design documentation; system configuration settings and associated documentation; system audit records; system monitoring records; system security plan; other relevant documents or records].
	AC-17(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].

AC-17(01)	REMOTE ACCESS | MONITORING AND CONTROL	
	AC-17(01)-Test	[SELECT FROM: Automated mechanisms monitoring and controlling remote access methods].

AC-17(02)	REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-17(02)	cryptographic mechanisms are implemented to protect the confidentiality and integrity of remote access sessions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-17(02)-Examine	[SELECT FROM: Access control policy; procedures addressing remote access to the system; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; system audit records; system security plan; other relevant documents or records].
	AC-17(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-17(02)-Test	[SELECT FROM: Cryptographic mechanisms protecting confidentiality and integrity of remote access sessions].

AC-17(03)	REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-17(03)	remote accesses are routed through authorized and managed network access control points.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-17(03)-Examine	[SELECT FROM: Access control policy; procedures addressing remote access to the system; system design documentation; list of all managed network access control points; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-17(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	AC-17(03)-Test	[SELECT FROM: Mechanisms routing all remote accesses through managed network access control points].

AC-17(04)	REMOTE ACCESS | PRIVILEGED COMMANDS AND ACCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-17(04)_ODP[01]	***needs requiring execution of privileged commands via remote access are defined;***
	AC-17(04)_ODP[02]	***needs requiring access to security-relevant information via remote access are defined;***
	AC-17(04)(a)[01]	the execution of privileged commands via remote access is authorized only in a format that provides assessable evidence;
	AC-17(04)(a)[02]	access to security-relevant information via remote access is authorized only in a format that provides assessable evidence;
	AC-17(04)(a)[03]	the execution of privileged commands via remote access is authorized only for the following needs: ***<AC-17(04)_ODP[01] needs requiring remote access>***;
	AC-17(04)(a)[04]	access to security-relevant information via remote access is authorized only for the following needs: ***<AC-17(04)_ODP[02] needs requiring remote access>***;
	AC-17(04)(b)	the rationale for remote access is documented in the security plan for the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-17(04)-Examine	[SELECT FROM: Access control policy; procedures addressing remote access to the system; system configuration settings and associated documentation; security plan; system audit records; system security plan; other relevant documents or records].
	AC-17(04)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	AC-17(04)-Test	[SELECT FROM: Mechanisms implementing remote access management].

AC-17(05)	REMOTE ACCESS | MONITORING FOR UNAUTHORIZED CONNECTIONS
	[WITHDRAWN: Incorporated into SI-04.]

AC-17(06)	REMOTE ACCESS | PROTECTION OF MECHANISM INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-17(06)	information about remote access mechanisms is protected from unauthorized use and disclosure.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-17(06)-Examine	[SELECT FROM: Access control policy; procedures addressing remote access to the system; system security plan; other relevant documents or records].
	AC-17(06)-Interview	[SELECT FROM: Organizational personnel with responsibilities for implementing or monitoring remote access to the system; system users with knowledge of information about remote access mechanisms; organizational personnel with information security responsibilities].

AC-17(07)	REMOTE ACCESS | ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS
	[WITHDRAWN: Incorporated into AC-03(10).]

AC-17(08)	REMOTE ACCESS | DISABLE NONSECURE NETWORK PROTOCOLS
	[WITHDRAWN: Incorporated into CM-07.]

AC-17(09)	REMOTE ACCESS | DISCONNECT OR DISABLE ACCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-17(09)_ODP	***the time period within which to disconnect or disable remote access to the system is defined;***
	AC-17(09)	the capability to disconnect or disable remote access to the system within ***<AC-17(09)_ODP time period>*** is provided.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-17(09)-Examine	[SELECT FROM: Access control policy; procedures addressing disconnecting or disabling remote access to the system; system design documentation; system configuration settings and associated documentation; security plan, system audit records; system security plan; other relevant documents or records].
	AC-17(09)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-17(09)-Test	[SELECT FROM: Mechanisms implementing capability to disconnect or disable remote access to system].

AC-17(10)	REMOTE ACCESS | AUTHENTICATE REMOTE COMMANDS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-17(10)_ODP[01]	***mechanisms implemented to authenticate remote commands are defined;***
	AC-17(10)_ODP[02]	***remote commands to be authenticated by mechanisms are defined;***
	AC-17(10)	***<AC-17(10)_ODP[01] mechanisms>*** are implemented to authenticate ***<AC-17(10)_ODP[02] remote commands>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-17(10)-Examine	[SELECT FROM: Access control policy; procedures addressing authentication of remote commands; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-17(10)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].

AC-17(10)	REMOTE ACCESS | AUTHENTICATE REMOTE COMMANDS	
	AC-17(10)-Test	[SELECT FROM: Mechanisms implementing authentication of remote commands].

AC-18	WIRELESS ACCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-18a.[01]	configuration requirements are established for each type of wireless access;
	AC-18a.[02]	connection requirements are established for each type of wireless access;
	AC-18a.[03]	implementation guidance is established for each type of wireless access;
	AC-18b.	each type of wireless access to the system is authorized prior to allowing such connections.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-18-Examine	[SELECT FROM: Access control policy; procedures addressing wireless access implementation and usage (including restrictions); configuration management plan; system design documentation; system configuration settings and associated documentation; wireless access authorizations; system audit records; system security plan; other relevant documents or records].
	AC-18-Interview	[SELECT FROM: Organizational personnel with responsibilities for managing wireless access connections; organizational personnel with information security responsibilities].
	AC-18-Test	[SELECT FROM: Wireless access management capability for the system].

AC-18(01)	WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-18(01)_ODP	***one or more of the following PARAMETER VALUES is/are selected: {users; devices};***
	AC-18(01)[01]	wireless access to the system is protected using authentication of ***<AC-18(01)_ODP SELECTED PARAMETER VALUE(S)>***;
	AC-18(01)[02]	wireless access to the system is protected using encryption.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-18(01)-Examine	[SELECT FROM: Access control policy; procedures addressing wireless implementation and usage (including restrictions); system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-18(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].

AC-18(01)	WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION	
	AC-18(01)-Test	[SELECT FROM: Mechanisms implementing wireless access protections to the system].

AC-18(02)	WIRELESS ACCESS | MONITORING UNAUTHORIZED CONNECTIONS	
	[WITHDRAWN: Incorporated into SI-04.]	

AC-18(03)	WIRELESS ACCESS | DISABLE WIRELESS NETWORKING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-18(03)	when not intended for use, wireless networking capabilities embedded within system components are disabled prior to issuance and deployment.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-18(03)-Examine	[SELECT FROM: Access control policy; procedures addressing wireless implementation and usage (including restrictions); system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-18(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	AC-18(03)-Test	[SELECT FROM: Mechanisms managing the disabling of wireless networking capabilities internally embedded within system components].

AC-18(04)	WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-18(04)[01]	users allowed to independently configure wireless networking capabilities are identified;
	AC-18(04)[02]	users allowed to independently configure wireless networking capabilities are explicitly authorized.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-18(04)-Examine	[SELECT FROM: Access control policy; procedures addressing wireless implementation and usage (including restrictions); system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-18(04)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	AC-18(04)-Test	[SELECT FROM: Mechanisms authorizing independent user configuration of wireless networking capabilities].

AC-18(05)	WIRELESS ACCESS | ANTENNAS AND TRANSMISSION POWER LEVELS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-18(05)[01]	radio antennas are selected to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries;
	AC-18(05)[02]	transmission power levels are calibrated to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-18(05)-Examine	[SELECT FROM: Access control policy; procedures addressing wireless implementation and usage (including restrictions); system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-18(05)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	AC-18(05)-Test	[SELECT FROM: Calibration of transmission power levels for wireless access; radio antenna signals for wireless access; wireless access reception outside of organization-controlled boundaries].

AC-19	ACCESS CONTROL FOR MOBILE DEVICES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-19a.[01]	configuration requirements are established for organization-controlled mobile devices, including when such devices are outside of the controlled area;
	AC-19a.[02]	connection requirements are established for organization-controlled mobile devices, including when such devices are outside of the controlled area;
	AC-19a.[03]	implementation guidance is established for organization-controlled mobile devices, including when such devices are outside of the controlled area;
	AC-19b.	the connection of mobile devices to organizational systems is authorized.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-19-Examine	[SELECT FROM: Access control policy; procedures addressing access control for mobile device usage (including restrictions); configuration management plan; system design documentation; system configuration settings and associated documentation; authorizations for mobile device connections to organizational systems; system audit records; system security plan; other relevant documents or records].
	AC-19-Interview	[SELECT FROM: Organizational personnel using mobile devices to access organizational systems; system/network administrators; organizational personnel with information security responsibilities].
	AC-19-Test	[SELECT FROM: Access control capability for mobile device connections to organizational systems; configurations of mobile devices].

AC-19(01)	ACCESS CONTROL FOR MOBILE DEVICES | USE OF WRITABLE AND PORTABLE STORAGE DEVICES
	[WITHDRAWN: Incorporated into MP-07.]

AC-19(02)	ACCESS CONTROL FOR MOBILE DEVICES | USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES
	[WITHDRAWN: Incorporated into MP-07.]

AC-19(03)	ACCESS CONTROL FOR MOBILE DEVICES | USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER
	[WITHDRAWN: Incorporated into MP-07.]

AC-19(04)	ACCESS CONTROL FOR MOBILE DEVICES | RESTRICTIONS FOR CLASSIFIED INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-19(04)_ODP[01]	***security officials responsible for the review and inspection of unclassified mobile devices and the information stored on those devices are defined;***
	AC-19(04)_ODP[02]	***security policies restricting the connection of classified mobile devices to classified systems are defined;***
	AC-19(04)(a)	the use of unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information is prohibited unless specifically permitted by the authorizing official;
	AC-19(04)(b)(01)	prohibition of the connection of unclassified mobile devices to classified systems is enforced on individuals permitted by an authorizing official to use unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information;
	AC-19(04)(b)(02)	approval by the authorizing official for the connection of unclassified mobile devices to unclassified systems is enforced on individuals permitted to use unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information;
	AC-19(04)(b)(03)	prohibition of the use of internal or external modems or wireless interfaces within unclassified mobile devices is enforced on individuals permitted by an authorizing official to use unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information;
	AC-19(04)(b)(04)[01]	random review and inspection of unclassified mobile devices and the information stored on those devices by ***<AC-19(04)_ODP[01] security officials>*** are enforced;
	AC-19(04)(b)(04)[02]	following of the incident handling policy is enforced if classified information is found during a random review and inspection of unclassified mobile devices;
	AC-19(04)(c)	the connection of classified mobile devices to classified systems is restricted in accordance with ***<AC-19(04)_ODP[02] security policies>***.

AC-19(04)	ACCESS CONTROL FOR MOBILE DEVICES | RESTRICTIONS FOR CLASSIFIED INFORMATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-19(04)-Examine	[SELECT FROM: Access control policy; incident handling policy; procedures addressing access control for mobile devices; system design documentation; system configuration settings and associated documentation; evidentiary documentation for random inspections and reviews of mobile devices; system audit records; system security plan; other relevant documents or records].
	AC-19(04)-Interview	[SELECT FROM: Organizational personnel responsible for random reviews/ inspections of mobile devices; organizational personnel using mobile devices in facilities containing systems processing, storing, or transmitting classified information; organizational personnel with incident response responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	AC-19(04)-Test	[SELECT FROM: Mechanisms prohibiting the use of internal or external modems or wireless interfaces with mobile devices].

AC-19(05)	ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE OR CONTAINER-BASED ENCRYPTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-19(05)_ODP[01]	***one of the following PARAMETER VALUES is selected: {full-device encryption; container-based encryption};***
	AC-19(05)_ODP[02]	***mobile devices on which to employ encryption are defined;***
	AC-19(05)	***<AC-19(05)_ODP[01] SELECTED PARAMETER VALUE>*** is employed to protect the confidentiality and integrity of information on ***<AC-19(05)_ODP[02] mobile devices>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-19(05)-Examine	[SELECT FROM: Access control policy; procedures addressing access control for mobile devices; system design documentation; system configuration settings and associated documentation; encryption mechanisms and associated configuration documentation; system audit records; system security plan; other relevant documents or records].
	AC-19(05)-Interview	[SELECT FROM: Organizational personnel with access control responsibilities for mobile devices; system/network administrators; organizational personnel with information security responsibilities].
	AC-19(05)-Test	[SELECT FROM: Encryption mechanisms protecting confidentiality and integrity of information on mobile devices].

AC-20	USE OF EXTERNAL SYSTEMS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-20_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {establish <AC-20_ODP[02] terms and conditions>; identify <AC-20_ODP[03] controls asserted>};***
	AC-20_ODP[02]	***terms and conditions consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems are defined (if selected);***
	AC-20_ODP[03]	***controls asserted to be implemented on external systems consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems are defined (if selected);***
	AC-20_ODP[04]	***types of external systems prohibited from use are defined;***
	AC-20a.1	***<AC-20_ODP[01] SELECTED PARAMETER VALUE(S)>*** is/are consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to access the system from external systems (if applicable);
	AC-20a.2	***<AC-20_ODP[01] SELECTED PARAMETER VALUE(S)>*** is/are consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to process, store, or transmit organization-controlled information using external systems (if applicable);
	AC-20b.	the use of ***<AC-20_ODP[04] prohibited types of external systems>*** is prohibited (if applicable).
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-20-Examine	[SELECT FROM: Access control policy; procedures addressing the use of external systems; external systems terms and conditions; list of types of applications accessible from external systems; maximum security categorization for information processed, stored, or transmitted on external systems; system configuration settings and associated documentation; system security plan; other relevant documents or records].
	AC-20-Interview	[SELECT FROM: Organizational personnel with responsibilities for defining terms and conditions for use of external systems to access organizational systems; system/network administrators; organizational personnel with information security responsibilities].
	AC-20-Test	[SELECT FROM: Mechanisms implementing terms and conditions on the use of external systems].

AC-20(01)	USE OF EXTERNAL SYSTEMS | LIMITS ON AUTHORIZED USE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-20(01)(a)	authorized individuals are permitted to use an external system to access the system or to process, store, or transmit organization-controlled information only after verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans (if applicable);

AC-20(01)	USE OF EXTERNAL SYSTEMS | LIMITS ON AUTHORIZED USE	
	AC-20(01)(b)	authorized individuals are permitted to use an external system to access the system or to process, store, or transmit organization-controlled information only after retention of approved system connection or processing agreements with the organizational entity hosting the external system (if applicable).
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-20(01)-Examine	[SELECT FROM: Access control policy; procedures addressing the use of external systems; system connection or processing agreements; account management documents; system security plan; other relevant documents or records].
	AC-20(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	AC-20(01)-Test	[SELECT FROM: Mechanisms implementing limits on use of external systems].

AC-20(02)	USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES — RESTRICTED USE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-20(02)_ODP	***restrictions on the use of organization-controlled portable storage devices by authorized individuals on external systems are defined;***
	AC-20(02)	the use of organization-controlled portable storage devices by authorized individuals is restricted on external systems using ***<AC-20(02)_ODP restrictions>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-20(02)-Examine	[SELECT FROM: Access control policy; procedures addressing the use of external systems; system configuration settings and associated documentation; system connection or processing agreements; account management documents; system security plan; other relevant documents or records].
	AC-20(02)-Interview	[SELECT FROM: Organizational personnel with responsibilities for restricting or prohibiting the use of organization-controlled storage devices on external systems; system/network administrators; organizational personnel with information security responsibilities].
	AC-20(02)-Test	[SELECT FROM: Mechanisms implementing restrictions on the use of portable storage devices].

AC-20(03)	USE OF EXTERNAL SYSTEMS | NON-ORGANIZATIONALLY OWNED SYSTEMS — RESTRICTED USE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-20(03)_ODP	***restrictions on the use of non-organizationally owned systems or system components to process, store, or transmit organizational information are defined;***
	AC-20(03)	the use of non-organizationally owned systems or system components to process, store, or transmit organizational information is restricted using ***<AC-20(03)_ODP restrictions>***.

AC-20(03)	USE OF EXTERNAL SYSTEMS | NON-ORGANIZATIONALLY OWNED SYSTEMS — RESTRICTED USE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-20(03)-Examine	[SELECT FROM: Access control policy; procedures addressing the use of external systems; system design documentation; system configuration settings and associated documentation; system connection or processing agreements; account management documents; system audit records, other relevant documents or records].
	AC-20(03)-Interview	[SELECT FROM: Organizational personnel with responsibilities for restricting or prohibiting the use of non-organizationally owned systems, system components, or devices; system/network administrators; organizational personnel with information security responsibilities].
	AC-20(03)-Test	[SELECT FROM: Mechanisms implementing restrictions on the use of non-organizationally owned systems, components, or devices].

AC-20(04)	USE OF EXTERNAL SYSTEMS | NETWORK ACCESSIBLE STORAGE DEVICES — PROHIBITED USE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-20(04)_ODP	***network-accessible storage devices prohibited from use in external systems are defined;***
	AC-20(04)	the use of ***<AC-20(04)_ODP network-accessible storage devices>*** is prohibited in external systems.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-20(04)-Examine	[SELECT FROM: Access control policy; procedures addressing use of network-accessible storage devices in external systems; system design documentation; system configuration settings and associated documentation; system connection or processing agreements; list of network-accessible storage devices prohibited from use in external systems; system audit records; system security plan; other relevant documents or records].
	AC-20(04)-Interview	[SELECT FROM: Organizational personnel with responsibilities for prohibiting the use of network-accessible storage devices in external systems; system/network administrators; organizational personnel with information security responsibilities].
	AC-20(04)-Test	[SELECT FROM: Mechanisms prohibiting the use of network-accessible storage devices in external systems].

AC-20(05)	USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES — PROHIBITED USE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-20(05)	the use of organization-controlled portable storage devices by authorized individuals is prohibited on external systems.

AC-20(05)	USE OF EXTERNAL SYSTEMS | PORTABLE STORAGE DEVICES — PROHIBITED USE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-20(05)-Examine	[SELECT FROM: Access control policy; procedures addressing use of portable storage devices in external systems; system design documentation; system configuration settings and associated documentation; system connection or processing agreements; system audit records; system security plan; other relevant documents or records].
	AC-20(05)-Interview	[SELECT FROM: Organizational personnel with responsibilities for prohibiting the use of portable storage devices in external systems; system/network administrators; organizational personnel with information security responsibilities].

AC-21	INFORMATION SHARING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-21_ODP[01]	***information-sharing circumstances where user discretion is required to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions are defined;***
	AC-21_ODP[02]	***automated mechanisms or manual processes that assist users in making information-sharing and collaboration decisions are defined;***
	AC-21a.	authorized users are enabled to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for ***<AC-21_ODP[01] information-sharing circumstances>***;
	AC-21b.	***<AC-21_ODP[02] automated mechanisms>*** are employed to assist users in making information-sharing and collaboration decisions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-21-Examine	[SELECT FROM: Access control policy; procedures addressing user-based collaboration and information sharing (including restrictions); system design documentation; system configuration settings and associated documentation; list of users authorized to make information-sharing/collaboration decisions; list of information-sharing circumstances requiring user discretion; non-disclosure agreements; acquisitions/contractual agreements; system security plan; privacy plan; privacy impact assessment; security and privacy risk assessments; other relevant documents or records].
	AC-21-Interview	[SELECT FROM: Organizational personnel responsible for information-sharing/collaboration decisions; organizational personnel with responsibility for acquisitions/contractual agreements; system/network administrators; organizational personnel with information security and privacy responsibilities].
	AC-21-Test	[SELECT FROM: Automated mechanisms or manual process implementing access authorizations supporting information-sharing/user collaboration decisions].

AC-21(01)	INFORMATION SHARING | AUTOMATED DECISION SUPPORT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-21(01)_ODP	***automated mechanisms employed to enforce information-sharing decisions by authorized users are defined;***
	AC-21(01)	***<AC-21(01)_ODP automated mechanisms>*** are employed to enforce information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-21(01)-Examine	[SELECT FROM: Access control policy; procedures addressing user-based collaboration and information sharing (including restrictions); system design documentation; system configuration settings and associated documentation; system-generated list of users authorized to make information-sharing/ collaboration decisions; system-generated list of sharing partners and access authorizations; system-generated list of access restrictions regarding information to be shared; system security plan; other relevant documents or records].
	AC-21(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-21(01)-Test	[SELECT FROM: Automated mechanisms implementing access authorizations supporting information-sharing/user collaboration decisions].

AC-21(02)	INFORMATION SHARING | INFORMATION SEARCH AND RETRIEVAL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-21(02)_ODP	***information-sharing restrictions to be enforced by information search and retrieval services are defined;***
	AC-21(02)	information search and retrieval services that enforce ***<AC-21(02)_ODP information-sharing restrictions>*** are implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-21(02)-Examine	[SELECT FROM: Access control policy; procedures addressing user-based collaboration and information sharing (including restrictions); system design documentation; system configuration settings and associated documentation; system-generated list of access restrictions regarding information to be shared; information search and retrieval records; system audit records; system security plan; other relevant documents or records].
	AC-21(02)-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities for system search and retrieval services; system/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-21(02)-Test	[SELECT FROM: System search and retrieval services enforcing information-sharing restrictions].

AC-22	PUBLICLY ACCESSIBLE CONTENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-22_ODP	***the frequency at which to review the content on the publicly accessible system for non-public information is defined;***
	AC-22a.	designated individuals are authorized to make information publicly accessible;
	AC-22b.	authorized individuals are trained to ensure that publicly accessible information does not contain non-public information;
	AC-22c.	the proposed content of information is reviewed prior to posting onto the publicly accessible system to ensure that non-public information is not included;
	AC-22d.[01]	the content on the publicly accessible system is reviewed for non-public information ***<AC-22_ODP frequency>***;
	AC-22d.[02]	non-public information is removed from the publicly accessible system, if discovered.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-22-Examine	[SELECT FROM: Access control policy; procedures addressing publicly accessible content; list of users authorized to post publicly accessible content on organizational systems; training materials and/or records; records of publicly accessible information reviews; records of response to non-public information on public websites; system audit logs; security awareness training records; system security plan; other relevant documents or records].
	AC-22-Interview	[SELECT FROM: Organizational personnel with responsibilities for managing publicly accessible information posted on organizational systems; organizational personnel with information security responsibilities].
	AC-22-Test	[SELECT FROM: Mechanisms implementing management of publicly accessible content].

AC-23	DATA MINING PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-23_ODP[01]	***data mining prevention and detection techniques are defined;***
	AC-23_ODP[02]	***data storage objects to be protected against unauthorized data mining are defined;***
	AC-23	***<AC-23_ODP[01] techniques>*** are employed for ***<AC-23_ODP[02] data storage objects>*** to detect and protect against unauthorized data mining.

AC-23	DATA MINING PROTECTION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-23-Examine	[SELECT FROM: Access control policy; procedures for preventing and detecting data mining; policies and procedures addressing authorized data mining techniques; procedures addressing protection of data storage objects against data mining; system design documentation; system configuration settings and associated documentation; system audit logs; system audit records; procedures addressing differential privacy techniques; notifications of atypical database queries or accesses; documentation or reports of insider threat program; system security plan; privacy plan; other relevant documents or records].
	AC-23-Interview	[SELECT FROM: Organizational personnel with responsibilities for implementing data mining detection and prevention techniques for data storage objects; legal counsel; organizational personnel with information security and privacy responsibilities; system developers].
	AC-23-Test	[SELECT FROM: Mechanisms implementing data mining prevention and detection].

AC-24	ACCESS CONTROL DECISIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-24_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {establish procedures; implement mechanisms};***
	AC-24_ODP[02]	***access control decisions applied to each access request prior to access enforcement are defined;***
	AC-24	***<AC-24_ODP[01] SELECTED PARAMETER VALUE(S)>*** are taken to ensure that ***<AC-24_ODP[02] access control decisions>*** are applied to each access request prior to access enforcement.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-24-Examine	[SELECT FROM: Access control policy; procedures addressing access control decisions; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-24-Interview	[SELECT FROM: Organizational personnel with responsibilities for establishing procedures regarding access control decisions to the system; organizational personnel with information security responsibilities].
	AC-24-Test	[SELECT FROM: Mechanisms applying established access control decisions and procedures].

AC-24(01)	ACCESS CONTROL DECISIONS | TRANSMIT ACCESS AUTHORIZATION INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-24(01)_ODP[01]	***access authorization information transmitted to systems that enforce access control decisions is defined;***

AC-24(01)	ACCESS CONTROL DECISIONS | TRANSMIT ACCESS AUTHORIZATION INFORMATION	
	AC-24(01)_ODP[02]	***controls to be used when authorization information is transmitted to systems that enforce access control decisions are defined;***
	AC-24(01)_ODP[03]	***systems that enforce access control decisions are defined;***
	AC-24(01)	***<AC-24(01)_ODP[01] access authorization information>*** is transmitted using ***<AC-24(01)_ODP[02] controls>*** to ***<AC-24(01)_ODP[03] systems>*** that enforce access control decisions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-24(01)-Examine	[SELECT FROM: Access control policy; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-24(01)-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-24(01)-Test	[SELECT FROM: Mechanisms implementing access enforcement functions].

AC-24(02)	ACCESS CONTROL DECISIONS | NO USER OR PROCESS IDENTITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-24(02)_ODP[01]	***security attributes that do not include the identity of the user or process acting on behalf of the user are defined (if selected);***
	AC-24(02)_ODP[02]	***privacy attributes that do not include the identity of the user or process acting on behalf of the user are defined (if selected);***
	AC-24(02)[01]	access control decisions are enforced based on ***<AC-24(02)_ODP[01] security attributes>*** that do not include the identity of the user or process acting on behalf of the user (if selected);
	AC-24(02)[02]	access control decisions are enforced based on ***<AC-24(02)_ODP[02] privacy attributes>*** that do not include the identity of the user or process acting on behalf of the user (if selected).
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-24(02)-Examine	[SELECT FROM: Access control policy; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; other relevant documents or records].
	AC-24(02)-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security and privacy responsibilities; system developers].
	AC-24(02)-Test	[SELECT FROM: Mechanisms implementing access enforcement functions].

AC-25	REFERENCE MONITOR	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AC-25_ODP	***access control policies for which a reference monitor is implemented are defined;***
	AC-25	a reference monitor is implemented for ***<AC-25_ODP access control policies>*** that is tamper-proof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-25-Examine	[SELECT FROM: Access control policy; procedures addressing access enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	AC-25-Interview	[SELECT FROM: Organizational personnel with access enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers].
	AC-25-Test	[SELECT FROM: Mechanisms implementing access enforcement functions].

4.2 AWARENESS AND TRAINING

AT-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AT-01_ODP[01]	***personnel or roles to whom the awareness and training policy is to be disseminated is/are defined;***
	AT-01_ODP[02]	***personnel or roles to whom the awareness and training procedures are to be disseminated is/are defined;***
	AT-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	AT-01_ODP[04]	***an official to manage the awareness and training policy and procedures is defined;***
	AT-01_ODP[05]	***the frequency at which the current awareness and training policy is reviewed and updated is defined;***
	AT-01_ODP[06]	***events that would require the current awareness and training policy to be reviewed and updated are defined;***
	AT-01_ODP[07]	***the frequency at which the current awareness and training procedures are reviewed and updated is defined;***
	AT-01_ODP[08]	***events that would require procedures to be reviewed and updated are defined;***
	AT-01a.[01]	an awareness and training policy is developed and documented;
	AT-01a.[02]	the awareness and training policy is disseminated to ***<AT-01_ODP[01] personnel or roles>***;
	AT-01a.[03]	awareness and training procedures to facilitate the implementation of the awareness and training policy and associated access controls are developed and documented;
	AT-01a.[04]	the awareness and training procedures are disseminated to ***<AT-01_ODP[02] personnel or roles>***.
	AT-01a.01(a)[01]	the ***<AT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** awareness and training policy addresses purpose;
	AT-01a.01(a)[02]	the ***<AT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** awareness and training policy addresses scope;
	AT-01a.01(a)[03]	the ***<AT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** awareness and training policy addresses roles;
	AT-01a.01(a)[04]	the ***<AT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** awareness and training policy addresses responsibilities;
	AT-01a.01(a)[05]	the ***<AT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** awareness and training policy addresses management commitment;
	AT-01a.01(a)[06]	the ***<AT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** awareness and training policy addresses coordination among organizational entities;
	AT-01a.01(a)[07]	the ***<AT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** awareness and training policy addresses compliance; and

AT-01	POLICY AND PROCEDURES	
	AT-01a.01(b)	the ***<AT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** awareness and training policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines; and
	AT-01b.	the ***<AT-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the awareness and training policy and procedures;
	AT-01c.01[01]	the current awareness and training policy is reviewed and updated ***<AT-01_ODP[05] frequency>***;
	AT-01c.01[02]	the current awareness and training policy is reviewed and updated following ***<AT-01_ODP[06] events>***;
	AT-01c.02[01]	the current awareness and training procedures are reviewed and updated ***<AT-01_ODP[07] frequency>***;
	AT-01c.02[02]	the current awareness and training procedures are reviewed and updated following ***<AT-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AT-01-Examine	[SELECT FROM: System security plan; privacy plan; awareness and training policy and procedures; other relevant documents or records].
	AT-01-Interview	[SELECT FROM: Organizational personnel with awareness and training responsibilities; organizational personnel with information security and privacy responsibilities].

AT-02	LITERACY TRAINING AND AWARENESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AT-02_ODP[01]	***the frequency at which to provide security literacy training to system users (including managers, senior executives, and contractors) after initial training is defined;***
	AT-02_ODP[02]	***the frequency at which to provide privacy literacy training to system users (including managers, senior executives, and contractors) after initial training is defined;***
	AT-02_ODP[03]	***events that require security literacy training for system users are defined;***
	AT-02_ODP[04]	***events that require privacy literacy training for system users are defined;***
	AT-02_ODP[05]	***techniques to be employed to increase the security and privacy awareness of system users are defined;***
	AT-02_ODP[06]	***the frequency at which to update literacy training and awareness content is defined;***
	AT-02_ODP[07]	***events that would require literacy training and awareness content to be updated are defined;***
	AT-02a.01[01]	security literacy training is provided to system users (including managers, senior executives, and contractors) as part of initial training for new users;

AT-02	LITERACY TRAINING AND AWARENESS	
	AT-02a.01[02]	privacy literacy training is provided to system users (including managers, senior executives, and contractors) as part of initial training for new users;
	AT-02a.01[03]	security literacy training is provided to system users (including managers, senior executives, and contractors) ***<AT-02_ODP[01] frequency>*** thereafter;
	AT-02a.01[04]	privacy literacy training is provided to system users (including managers, senior executives, and contractors) ***<AT-02_ODP[02] frequency>*** thereafter;
	AT-02a.02[01]	security literacy training is provided to system users (including managers, senior executives, and contractors) when required by system changes or following ***<AT-02_ODP[03] events>***;
	AT-02a.02[02]	privacy literacy training is provided to system users (including managers, senior executives, and contractors) when required by system changes or following ***<AT-02_ODP[04] events>***;
	AT-02b.	***<AT-02_ODP[05] awareness techniques>*** are employed to increase the security and privacy awareness of system users;
	AT-02c.[01]	literacy training and awareness content is updated ***<AT-02_ODP[06] frequency>***;
	AT-02c.[02]	literacy training and awareness content is updated following ***<AT-02_ODP[07] events>***;
	AT-02d.	lessons learned from internal or external security incidents or breaches are incorporated into literacy training and awareness techniques.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AT-02-Examine	[SELECT FROM: System security plan; privacy plan; literacy training and awareness policy; procedures addressing literacy training and awareness implementation; appropriate codes of federal regulations; security and privacy literacy training curriculum; security and privacy literacy training materials; training records; other relevant documents or records].
	AT-02-Interview	[SELECT FROM: Organizational personnel with responsibilities for literacy training and awareness; organizational personnel with information security and privacy responsibilities; organizational personnel comprising the general system user community].
	AT-02-Test	[SELECT FROM: Mechanisms managing information security and privacy literacy training].

AT-02(01)	LITERACY TRAINING AND AWARENESS | PRACTICAL EXERCISES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AT-02(01)	practical exercises in literacy training that simulate events and incidents are provided.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AT-02(01)-Examine	[SELECT FROM: System security plan; privacy plan; security awareness and training policy; procedures addressing security awareness training implementation; security awareness training curriculum; security awareness training materials; other relevant documents or records].

AT-02(01)	LITERACY TRAINING AND AWARENESS | PRACTICAL EXERCISES	
	AT-02(01)-Interview	[SELECT FROM: Organizational personnel who receive literacy training and awareness; organizational personnel with responsibilities for security awareness training; organizational personnel with information security responsibilities].
	AT-02(01)-Test	[SELECT FROM: Mechanisms implementing cyber-attack simulations in practical exercises].

AT-02(02)	LITERACY TRAINING AND AWARENESS | INSIDER THREAT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AT-02(02)[01]	literacy training on recognizing potential indicators of insider threat is provided;
	AT-02(02)[02]	literacy training on reporting potential indicators of insider threat is provided.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AT-02(02)-Examine	[SELECT FROM: System security plan; privacy plan; literacy training and awareness policy; procedures addressing literacy training and awareness implementation; literacy training and awareness curriculum; literacy training and awareness materials; other relevant documents or records].
	AT-02(02)-Interview	[SELECT FROM: Organizational personnel who receive literacy training and awareness; organizational personnel with responsibilities for literacy training and awareness; organizational personnel with information security and privacy responsibilities].

AT-02(03)	LITERACY TRAINING AND AWARENESS | SOCIAL ENGINEERING AND MINING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AT-02(03)[01]	literacy training on recognizing potential and actual instances of social engineering is provided;
	AT-02(03)[02]	literacy training on reporting potential and actual instances of social engineering is provided;
	AT-02(03)[03]	literacy training on recognizing potential and actual instances of social mining is provided;
	AT-02(03)[04]	literacy training on reporting potential and actual instances of social mining is provided.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AT-02(03)-Examine	[SELECT FROM: System security plan; privacy plan; literacy training and awareness policy; procedures addressing literacy training and awareness implementation; literacy training and awareness curriculum; literacy training and awareness materials; other relevant documents or records].

AT-02(03)	LITERACY TRAINING AND AWARENESS | SOCIAL ENGINEERING AND MINING	
	AT-02(03)-Interview	[SELECT FROM: Organizational personnel who receive literacy training and awareness; organizational personnel with responsibilities for literacy training and awareness; organizational personnel with information security and privacy responsibilities].

AT-02(04)	LITERACY TRAINING AND AWARENESS | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AT-02(04)_ODP	***indicators of malicious code are defined;***
	AT-02(04)	literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using ***<AT-02(04)_ODP indicators of malicious code>*** is provided.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AT-02(04)-Examine	[SELECT FROM: System security plan; privacy plan; literacy training and awareness policy; procedures addressing literacy training and awareness implementation; literacy training and awareness curriculum; literacy training and awareness materials; other relevant documents or records].
	AT-02(04)-Interview	[SELECT FROM: Organizational personnel who receive literacy training and awareness; organizational personnel with responsibilities for basic literacy training and awareness; organizational personnel with information security and privacy responsibilities].

AT-02(05)	LITERACY TRAINING AND AWARENESS | ADVANCED PERSISTENT THREAT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AT-02(05)	literacy training on the advanced persistent threat is provided.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AT-02(05)-Examine	[SELECT FROM: System security plan; privacy plan; literacy training and awareness policy; procedures addressing literacy training and awareness implementation; literacy training and awareness curriculum; literacy training and awareness materials; other relevant documents or records].
	AT-02(05)-Interview	[SELECT FROM: Organizational personnel who receive literacy training and awareness; organizational personnel with responsibilities for basic literacy training and awareness; organizational personnel with information security and privacy responsibilities].

AT-02(06)	LITERACY TRAINING AND AWARENESS | CYBER THREAT ENVIRONMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AT-02(06)(a)	literacy training on the cyber threat environment is provided;
	AT-02(06)(b)	system operations reflects current cyber threat information.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AT-02(06)-Examine	[SELECT FROM: System security plan; privacy plan; literacy training and awareness policy; procedures addressing literacy training and awareness training implementation; literacy training and awareness curriculum; literacy training and awareness materials; other relevant documents or records].
	AT-02(06)-Interview	[SELECT FROM: Organizational personnel who receive literacy training and awareness; organizational personnel with responsibilities for basic literacy training and awareness; organizational personnel with information security and privacy responsibilities].

AT-03	ROLE-BASED TRAINING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AT-03_ODP[01]	***roles and responsibilities for role-based security training are defined;***
	AT-03_ODP[02]	***roles and responsibilities for role-based privacy training are defined;***
	AT-03_ODP[03]	***the frequency at which to provide role-based security and privacy training to assigned personnel after initial training is defined;***
	AT-03_ODP[04]	***the frequency at which to update role-based training content is defined;***
	AT-03_ODP[05]	***events that require role-based training content to be updated are defined;***
	AT-03a.01[01]	role-based security training is provided to ***<AT-03_ODP[01] roles and responsibilities>*** before authorizing access to the system, information, or performing assigned duties;
	AT-03a.01[02]	role-based privacy training is provided to ***<AT-03_ODP[02] roles and responsibilities>*** before authorizing access to the system, information, or performing assigned duties;
	AT-03a.01[03]	role-based security training is provided to ***<AT-03_ODP[01] roles and responsibilities>*** ***<AT-03_ODP[03] frequency>*** thereafter;
	AT-03a.01[04]	role-based privacy training is provided to ***<AT-03_ODP[02] roles and responsibilities>*** ***<AT-03_ODP[03] frequency>*** thereafter;
	AT-03a.02[01]	role-based security training is provided to personnel with assigned security roles and responsibilities when required by system changes;
	AT-03a.02[02]	role-based privacy training is provided to personnel with assigned security roles and responsibilities when required by system changes;
	AT-03b.[01]	role-based training content is updated ***<AT-03_ODP[04] frequency>***;
	AT-03b.[02]	role-based training content is updated following ***<AT-03_ODP[05] events>***;

AT-03	ROLE-BASED TRAINING	
	AT-03c.	lessons learned from internal or external security incidents or breaches are incorporated into role-based training.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AT-03-Examine	[SELECT FROM: System security plan; privacy plan; security and privacy awareness and training policy; procedures addressing security and privacy training implementation; codes of federal regulations; security and privacy training curriculum; security and privacy training materials; training records; other relevant documents or records].
	AT-03-Interview	[SELECT FROM: Organizational personnel with responsibilities for role-based security and privacy training; organizational personnel with assigned system security and privacy roles and responsibilities].
	AT-03-Test	[SELECT FROM: Mechanisms managing role-based security and privacy training].

AT-03(01)	ROLE-BASED TRAINING | ENVIRONMENTAL CONTROLS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AT-03(01)_ODP[01]	***personnel or roles to be provided with initial and refresher training in the employment and operation of environmental controls are defined;***
	AT-03(01)_ODP[02]	***the frequency at which to provide refresher training in the employment and operation of environmental controls is defined;***
	AT-03(01)	***<AT-03(01)_ODP[01] personnel or roles>*** are provided with initial and refresher training ***<AT-03(01)_ODP[02] frequency>*** in the employment and operation of environmental controls.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AT-03(01)-Examine	[SELECT FROM: Security and privacy awareness and training policy; procedures addressing security and privacy training implementation; security and privacy training curriculum; security and privacy training materials; system security plan; privacy plan; training records; other relevant documents or records].
	AT-03(01)-Interview	[SELECT FROM: Organizational personnel with responsibilities for role-based security and privacy training; organizational personnel with responsibilities for employing and operating environmental controls].

AT-03(02)	ROLE-BASED TRAINING | PHYSICAL SECURITY CONTROLS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AT-03(02)_ODP[01]	***personnel or roles to be provided with initial and refresher training in the employment and operation of physical security controls is/are defined;***
	AT-03(02)_ODP[02]	***the frequency at which to provide refresher training in the employment and operation of physical security controls is defined;***

AT-03(02)	ROLE-BASED TRAINING | PHYSICAL SECURITY CONTROLS	
	AT-03(02)	***<AT-03(02)_ODP[01] personnel or roles>*** is/are provided with initial and refresher training ***<AT-03(02)_ODP[02] frequency>*** in the employment and operation of physical security controls.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AT-03(02)-Examine	[SELECT FROM: Security and privacy awareness and training policy; procedures addressing security and privacy training implementation; security and privacy training curriculum; security and privacy training materials; system security plan; privacy plan; training records; other relevant documents or records].
	AT-03(02)-Interview	[SELECT FROM: Organizational personnel with responsibilities for role-based security and privacy training; organizational personnel with responsibilities for employing and operating physical security controls].

AT-03(03)	ROLE-BASED TRAINING | PRACTICAL EXERCISES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AT-03(03)[01]	practical exercises in security training that reinforce training objectives are provided;
	AT-03(03)[02]	practical exercises in privacy training that reinforce training objectives are provided.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AT-03(03)-Examine	[SELECT FROM: Security and privacy awareness and training policy; procedures addressing security and privacy awareness training implementation; security and privacy awareness training curriculum; security and privacy awareness training materials; security and privacy awareness training reports and results; system security plan; privacy plan; other relevant documents or records].
	AT-03(03)-Interview	[SELECT FROM: Organizational personnel with responsibilities for role-based security and privacy training; organizational personnel who participate in security and privacy awareness training].

AT-03(04)	ROLE-BASED TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR	
	[WITHDRAWN: Moved to AT-02(04).]	

AT-03(05)	ROLE-BASED TRAINING | PROCESSING PERSONALLY IDENTIFIABLE INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AT-03(05)_ODP[01]	***personnel or roles to be provided with initial and refresher training in the employment and operation of personally identifiable information processing and transparency controls is/are defined;***

AT-03(05)	ROLE-BASED TRAINING | PROCESSING PERSONALLY IDENTIFIABLE INFORMATION	
	AT-03(05)_ODP[02]	***the frequency at which to provide refresher training in the employment and operation of personally identifiable information processing and transparency controls is defined;***
	AT-03(05)	***<AT-03(05)_ODP[01] personnel or roles>*** are provided with initial and refresher training ***<AT-03(05)_ODP[02] frequency>*** in the employment and operation of personally identifiable information processing and transparency controls.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AT-03(05)-Examine	[SELECT FROM: Security and privacy awareness and training policy; procedures addressing security and privacy awareness training implementation; security and privacy awareness training curriculum; security and privacy awareness training materials; system security plan; privacy plan; organizational privacy notices; organizational policies; system of records notices; Privacy Act statements; computer matching agreements and notices; privacy impact assessments; information sharing agreements; other relevant documents or records].
	AT-03(05)-Interview	[SELECT FROM: Organizational personnel with responsibilities for role-based security and privacy training; organizational personnel who participate in security and privacy awareness training].

AT-04	TRAINING RECORDS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AT-04_ODP	***time period for retaining individual training records is defined;***
	AT-04a.[01]	information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training, are documented;
	AT-04a.[02]	information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training, are monitored;
	AT-04b.	individual training records are retained for ***<AT-04_ODP time period>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AT-04-Examine	[SELECT FROM: Security and privacy awareness and training policy; procedures addressing security and privacy training records; security and privacy awareness and training records; system security plan; privacy plan; other relevant documents or records].
	AT-04-Interview	[SELECT FROM: Organizational personnel with information security and privacy training record retention responsibilities].
	AT-04-Test	[SELECT FROM: Mechanisms supporting the management of security and privacy training records].

AT-05	CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS
	[WITHDRAWN: Incorporated into PM-15.]

AT-06	TRAINING FEEDBACK	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AT-06_ODP[01]	***frequency at which to provide feedback on organizational training results is defined;***
	AT-06_ODP[02]	***personnel to whom feedback on organizational training results will be provided is/are assigned;***
	AT-06	feedback on organizational training results is provided ***<AT-06_ODP[01] frequency>*** to ***<AT-06_ODP[02] personnel>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AT-06-Examine	[SELECT FROM: Security awareness and training policy; procedures addressing security training records; security awareness and training records; security plan; other relevant documents or records].
	AT-06-Interview	[SELECT FROM: Organizational personnel with information security training record retention responsibilities].
	AT-06-Test	[SELECT FROM: Mechanisms supporting the management of security training records].

4.3 AUDIT AND ACCOUNTABILITY

AU-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-01_ODP[01]	***personnel or roles to whom the audit and accountability policy is to be disseminated is/are defined;***
	AU-01_ODP[02]	***personnel or roles to whom the audit and accountability procedures are to be disseminated is/are defined;***
	AU-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	AU-01_ODP[04]	***an official to manage the audit and accountability policy and procedures is defined;***
	AU-01_ODP[05]	***the frequency at which the current audit and accountability policy is reviewed and updated is defined;***
	AU-01_ODP[06]	***events that would require the current audit and accountability policy to be reviewed and updated are defined;***
	AU-01_ODP[07]	***the frequency at which the current audit and accountability procedures are reviewed and updated is defined;***
	AU-01_ODP[08]	***events that would require audit and accountability procedures to be reviewed and updated are defined;***
	AU-01a.[01]	an audit and accountability policy is developed and documented;
	AU-01a.[02]	the audit and accountability policy is disseminated to ***<AU-01_ODP[01] personnel or roles>***;
	AU-01a.[03]	audit and accountability procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls are developed and documented;
	AU-01a.[04]	the audit and accountability procedures are disseminated to ***<AU-01_ODP[02] personnel or roles>***;
	AU-01a.01(a)[01]	the ***<AU-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** of the audit and accountability policy addresses purpose;
	AU-01a.01(a)[02]	the ***<AU-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** of the audit and accountability policy addresses scope;
	AU-01a.01(a)[03]	the ***<AU-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** of the audit and accountability policy addresses roles;
	AU-01a.01(a)[04]	the ***<AU-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** of the audit and accountability policy addresses responsibilities;
	AU-01a.01(a)[05]	the ***<AU-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** of the audit and accountability policy addresses management commitment;
	AU-01a.01(a)[06]	the ***<AU-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** of the audit and accountability policy addresses coordination among organizational entities;

AU-01	POLICY AND PROCEDURES	
	AU-01a.01(a)[07]	the ***<AU-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** of the audit and accountability policy addresses compliance;
	AU-01a.01(b)	the ***<AU-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** of the audit and accountability policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines;
	AU-01b.	the ***<AU-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the audit and accountability policy and procedures;
	AU-01c.01[01]	the current audit and accountability policy is reviewed and updated ***<AU-01_ODP[05] frequency>***;
	AU-01c.01[02]	the current audit and accountability policy is reviewed and updated following ***<AU-01_ODP[06] events>***;
	AU-01c.02[01]	the current audit and accountability procedures are reviewed and updated ***<AU-01_ODP[07] frequency>***;
	AU-01c.02[02]	the current audit and accountability procedures are reviewed and updated following ***<AU-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-01-Examine	[SELECT FROM: Audit and accountability policy and procedures; system security plan; privacy plan; other relevant documents or records].
	AU-01-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities].

AU-02	EVENT LOGGING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-02_ODP[01]	***the event types that the system is capable of logging in support of the audit function are defined;***
	AU-02_ODP[02]	***the event types (subset of AU-02_ODP[01]) for logging within the system are defined;***
	AU-02_ODP[03]	***the frequency or situation requiring logging for each specified event type is defined;***
	AU-02_ODP[04]	***the frequency of event types selected for logging are reviewed and updated;***
	AU-02a.	***<AU-02_ODP[01] event types>*** that the system is capable of logging are identified in support of the audit logging function;
	AU-02b.	the event logging function is coordinated with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;
	AU-02c.[01]	***<AU-02_ODP[02] event types (subset of AU-02_ODP[01])>*** are specified for logging within the system;

AU-02	EVENT LOGGING	
	AU-02c.[02]	the specified event types are logged within the system ***<AU-02_ODP[03] frequency or situation>***;
	AU-02d.	a rationale is provided for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents;
	AU-02e.	the event types selected for logging are reviewed and updated ***<AU-02_ODP[04] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-02-Examine	[SELECT FROM: Audit and accountability policy; procedures addressing auditable events; system security plan; privacy plan; system design documentation; system configuration settings and associated documentation; system audit records; system auditable events; other relevant documents or records].
	AU-02-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	AU-02-Test	[SELECT FROM: Mechanisms implementing system auditing].

AU-02(01)	EVENT LOGGING | COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES
	[WITHDRAWN: Incorporated into AU-12.]

AU-02(02)	EVENT LOGGING | SELECTION OF AUDIT EVENTS BY COMPONENT
	[WITHDRAWN: Incorporated into AU-12.]

AU-02(03)	EVENT LOGGING | REVIEWS AND UPDATES
	[WITHDRAWN: Incorporated into AU-02.]

AU-02(04)	EVENT LOGGING | PRIVILEGED FUNCTIONS
	[WITHDRAWN: Incorporated into AC-06(09).]

AU-03	CONTENT OF AUDIT RECORDS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-03a.	audit records contain information that establishes what type of event occurred;

AU-03	CONTENT OF AUDIT RECORDS	
	AU-03b.	audit records contain information that establishes when the event occurred;
	AU-03c.	audit records contain information that establishes where the event occurred;
	AU-03d.	audit records contain information that establishes the source of the event;
	AU-03e.	audit records contain information that establishes the outcome of the event;
	AU-03f.	audit records contain information that establishes the identity of any individuals, subjects, or objects/entities associated with the event.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-03-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing content of audit records; system design documentation; system configuration settings and associated documentation; list of organization-defined auditable events; system audit records; system incident reports; other relevant documents or records].
	AU-03-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	AU-03-Test	[SELECT FROM: Mechanisms implementing system auditing of auditable events].

AU-03(01)	CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-03(01)_ODP	***additional information to be included in audit records is defined;***
	AU-03(01)	generated audit records contain the following ***<AU-03(01)_ODP additional information>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-03(01)-Examine	[SELECT FROM: Audit and accountability policy; procedures addressing content of audit records; system security plan; privacy plan; system design documentation; system configuration settings and associated documentation; list of organization-defined auditable events; system audit records; other relevant documents or records].
	AU-03(01)-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-03(01)-Test	[SELECT FROM: system audit capability].

AU-03(02)	CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT
	[WITHDRAWN: Incorporated into PL-09.]

AU-03(03)	CONTENT OF AUDIT RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-03(03)_ODP	***elements identified in the privacy risk assessment are defined;***
	AU-03(03)	personally identifiable information contained in audit records is limited to ***<AU-03(03)_ODP elements>*** identified in the privacy risk assessment.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-03(03)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; privacy risk assessment; privacy risk assessment results; procedures addressing content of audit records; system design documentation; system configuration settings and associated documentation; list of organization-defined auditable events; system audit records; third party contracts; other relevant documents or records].
	AU-03(03)-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-03(03)-Test	[SELECT FROM: system audit capability].

AU-04	AUDIT LOG STORAGE CAPACITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-04_ODP	***audit log retention requirements are defined;***
	AU-04	audit log storage capacity is allocated to accommodate ***<AU-04_ODP audit log retention requirements>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-04-Examine	[SELECT FROM: Audit and accountability policy; procedures addressing audit storage capacity; system security plan; privacy plan; system design documentation; system configuration settings and associated documentation; audit record storage requirements; audit record storage capability for system components; system audit records; other relevant documents or records].
	AU-04-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-04-Test	[SELECT FROM: Audit record storage capacity and related configuration settings].

AU-04(01)	AUDIT LOG STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-04(01)_ODP	***the frequency of audit logs transferred to a different system, system component, or media other than the system or system component conducting the logging is defined;***
	AU-04(01)	audit logs are transferred ***<AU-04(01)_ODP frequency>*** to a different system, system component, or media other than the system or system component conducting the logging.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-04(01)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing audit storage capacity; procedures addressing transfer of system audit records to secondary or alternate systems; system design documentation; system configuration settings and associated documentation; logs of audit record transfers to secondary or alternate systems; system audit records transferred to secondary or alternate systems; other relevant documents or records].
	AU-04(01)-Interview	[SELECT FROM: Organizational personnel with audit storage capacity planning responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	AU-04(01)-Test	[SELECT FROM: Mechanisms supporting the transfer of audit records onto a different system].

AU-05	RESPONSE TO AUDIT LOGGING PROCESS FAILURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-05_ODP[01]	***personnel or roles receiving audit logging process failure alerts are defined;***
	AU-05_ODP[02]	***time period for personnel or roles receiving audit logging process failure alerts is defined;***
	AU-05_ODP[03]	***additional actions to be taken in the event of an audit logging process failure are defined;***
	AU-05a.	***<AU-05_ODP[01] personnel or roles>*** are alerted in the event of an audit logging process failure within ***<AU-05_ODP[02] time period>***;
	AU-05b.	***<AU-05_ODP[03] additional actions>*** are taken in the event of an audit logging process failure.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-05-Examine	[SELECT FROM: Audit and accountability policy; procedures addressing response to audit processing failures; system design documentation; system security plan; privacy plan; system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; system audit records; other relevant documents or records].

AU-05	RESPONSE TO AUDIT LOGGING PROCESS FAILURES	
	AU-05-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-05-Test	[SELECT FROM: Mechanisms implementing system response to audit processing failures].

AU-05(01)	RESPONSE TO AUDIT LOGGING PROCESS FAILURES | STORAGE CAPACITY WARNING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-05(01)_ODP[01]	***personnel, roles, and/or locations to be warned when allocated audit log storage volume reaches a percentage of repository maximum audit log storage capacity.***
	AU-05(01)_ODP[02]	***time period for defined personnel, roles, and/or locations to be warned when allocated audit log storage volume reaches a percentage of repository maximum audit log storage capacity is defined;***
	AU-05(01)_ODP[03]	***percentage of repository maximum audit log storage capacity is defined;***
	AU-05(01)	a warning is provided to ***<AU-05(01)_ODP[01] personnel, roles, and/or locations>*** within ***<AU-05(01)_ODP[02] time period>*** when allocated audit log storage volume reaches ***<AU-05(01)_ODP[03] percentage>*** of repository maximum audit log storage capacity.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-05(01)-Examine	[SELECT FROM: Audit and accountability policy; procedures addressing response to audit processing failures; system design documentation; system security plan; privacy system configuration settings and associated documentation; system audit records; other relevant documents or records].
	AU-05(01)-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-05(01)-Test	[SELECT FROM: Mechanisms implementing audit storage limit warnings].

AU-05(02)	RESPONSE TO AUDIT LOGGING PROCESS FAILURES | REAL-TIME ALERTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-05(02)_ODP[01]	***real-time period requiring alerts when audit failure events (defined in AU-05(02)_ODP[03]) occur is defined;***
	AU-05(02)_ODP[02]	***personnel, roles, and/or locations to be alerted in real time when audit failure events (defined in AU-05(02)_ODP[03]) occur is/are defined;***
	AU-05(02)_ODP[03]	***audit logging failure events requiring real-time alerts are defined;***

AU-05(02)	RESPONSE TO AUDIT LOGGING PROCESS FAILURES | REAL-TIME ALERTS	
	AU-05(02)	an alert is provided within ***<AU-05(02)_ODP[01] real-time period>*** to ***<AU-05(02)_ODP[02] personnel, roles, and/or locations>*** when ***<AU-05(02)_ODP[03] audit logging failure events requiring real-time alerts>*** occur.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-05(02)-Examine	[SELECT FROM: Audit and accountability policy; procedures addressing response to audit processing failures; system design documentation; system security plan; privacy plan; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	AU-05(02)-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].

AU-05(03)	RESPONSE TO AUDIT LOGGING PROCESS FAILURES | CONFIGURABLE TRAFFIC VOLUME THRESHOLDS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-05(03)_ODP	***one or more of the following PARAMETER VALUES is/are selected: {reject; delay};***
	AU-05(03)[01]	configurable network communications traffic volume thresholds reflecting limits on audit log storage capacity are enforced;
	AU-05(03)[02]	network traffic is ***<AU-05(03)_ODP SELECTED PARAMETER VALUE(S)>*** if network traffic volume is above configured thresholds.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-05(03)-Examine	[SELECT FROM: Audit and accountability policy; procedures addressing response to audit processing failures; system design documentation; system security plan; privacy plan; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	AU-05(03)-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].

AU-05(04)	RESPONSE TO AUDIT LOGGING PROCESS FAILURES | SHUTDOWN ON FAILURE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-05(04)_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {full system shutdown; partial system shutdown; degraded operational mode with limited mission or business functionality available};***
	AU-05(04)_ODP[02]	***audit logging failures that trigger a change in operational mode are defined;***

AU-05(04)	RESPONSE TO AUDIT LOGGING PROCESS FAILURES | SHUTDOWN ON FAILURE	
	AU-05(04)	***<AU-05(04)_ODP[01] SELECTED PARAMETER VALUE(S)>*** is/are invoked in the event of ***<AU-05(04)_ODP[02] audit logging failures>*** , unless an alternate audit logging capability exists.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-05(04)-Examine	[SELECT FROM: Audit and accountability policy; procedures addressing response to audit processing failures; system design documentation; system security plan; privacy plan; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	AU-05(04)-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-05(04)-Test	[SELECT FROM: System capability invoking system shutdown or degraded operational mode in the event of an audit processing failure].

AU-05(05)	RESPONSE TO AUDIT LOGGING PROCESS FAILURES | ALTERNATE AUDIT LOGGING CAPABILITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-05(05)_ODP	***an alternate audit logging functionality in the event of a failure in primary audit logging capability is defined;***
	AU-05(05)	an alternate audit logging capability is provided in the event of a failure in primary audit logging capability that implements ***<AU-05(05)_ODP alternate audit logging functionality>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-05(05)-Examine	[SELECT FROM: Audit and accountability policy; procedures addressing response to audit processing failures; system design documentation; system security plan; privacy plan; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	AU-05(05)-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-05(05)-Test	[SELECT FROM: Alternate audit logging capability].

AU-06	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-06_ODP[01]	***frequency at which system audit records are reviewed and analyzed is defined;***
	AU-06_ODP[02]	***inappropriate or unusual activity is defined;***

AU-06	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING	
	AU-06_ODP[03]	***personnel or roles to receive findings from reviews and analyses of system records is/are defined;***
	AU-06a.	system audit records are reviewed and analyzed ***<AU-06_ODP[01] frequency>*** for indications of ***<AU-06_ODP[02] inappropriate or unusual activity>*** and the potential impact of the inappropriate or unusual activity;
	AU-06b.	findings are reported to ***<AU-06_ODP[03] personnel or roles>***;
	AU-06c.	the level of audit record review, analysis, and reporting within the system is adjusted when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-06-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews/analyses of audit records; other relevant documents or records].
	AU-06-Interview	[SELECT FROM: Organizational personnel with audit review, analysis, and reporting responsibilities; organizational personnel with information security and privacy responsibilities].

AU-06(01)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | AUTOMATED PROCESS INTEGRATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-06(01)_ODP	***automated mechanisms used for integrating audit record review, analysis, and reporting processes are defined;***
	AU-06(01)	audit record review, analysis, and reporting processes are integrated using ***<AU-06(01)_ODP automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-06(01)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing audit review, analysis, and reporting; procedures addressing investigation and response to suspicious activities; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	AU-06(01)-Interview	[SELECT FROM: Organizational personnel with audit review, analysis, and reporting responsibilities; organizational personnel with information security and privacy responsibilities].
	AU-06(01)-Test	[SELECT FROM: Automated mechanisms integrating audit review, analysis, and reporting processes].

AU-06(02)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | AUTOMATED SECURITY ALERTS
	[WITHDRAWN: Incorporated into SI-04.]

AU-06(03)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT RECORD REPOSITORIES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-06(03)	audit records across different repositories are analyzed and correlated to gain organization-wide situational awareness.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-06(03)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing audit review, analysis, and reporting; system design documentation; system configuration settings and associated documentation; system audit records across different repositories; other relevant documents or records].
	AU-06(03)-Interview	[SELECT FROM: Organizational personnel with audit review, analysis, and reporting responsibilities; organizational personnel with information security and privacy responsibilities].
	AU-06(03)-Test	[SELECT FROM: Mechanisms supporting the analysis and correlation of audit records].

AU-06(04)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-06(04)[01]	the capability to centrally review and analyze audit records from multiple components within the system is provided;
	AU-06(04)[02]	the capability to centrally review and analyze audit records from multiple components within the system is implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-06(04)-Examine	[SELECT FROM: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; system design documentation; system configuration settings and associated documentation; system security plan; privacy plan; system audit records; other relevant documents or records].
	AU-06(04)-Interview	[SELECT FROM: Organizational personnel with audit review, analysis, and reporting responsibilities; organizational personnel with information security and privacy responsibilities; system developers].
	AU-06(04)-Test	[SELECT FROM: System capability to centralize review and analysis of audit records].

AU-06(05)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | INTEGRATED ANALYSIS OF AUDIT RECORDS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-06(05)_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {vulnerability scanning information; performance data; system monitoring information; <AU-06(05)_ODP[02] data/information collected from other sources>};***
	AU-06(05)_ODP[02]	***data/information collected from other sources to be analyzed is defined (if selected);***
	AU-06(05)	analysis of audit records is integrated with analysis of ***<AU-06(05)_ODP[01] SELECTED PARAMETER VALUE(S)>*** to further enhance the ability to identify inappropriate or unusual activity.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-06(05)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing audit review, analysis, and reporting; system design documentation; system configuration settings and associated documentation; integrated analysis of audit records, vulnerability scanning information, performance data, network monitoring information, and associated documentation; other relevant documents or records].
	AU-06(05)-Interview	[SELECT FROM: Organizational personnel with audit review, analysis, and reporting responsibilities; organizational personnel with information security and privacy responsibilities].
	AU-06(05)-Test	[SELECT FROM: Mechanisms implementing the capability to integrate analysis of audit records with analysis of data/information sources].

AU-06(06)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-06(06)	information from audit records is correlated with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-06(06)-Examine	[SELECT FROM: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; procedures addressing physical access monitoring; system design documentation; system configuration settings and associated documentation; documentation providing evidence of correlated information obtained from audit records and physical access monitoring records; system security plan; privacy plan; other relevant documents or records].
	AU-06(06)-Interview	[SELECT FROM: Organizational personnel with audit review, analysis, and reporting responsibilities; organizational personnel with physical access monitoring responsibilities; organizational personnel with information security and privacy responsibilities].

AU-06(06)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING	
	AU-06(06)-Test	[SELECT FROM: Mechanisms implementing the capability to correlate information from audit records with information from monitoring physical access].

AU-06(07)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | PERMITTED ACTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-06(07)_ODP	***one or more of the following PARAMETER VALUES is/are selected: {system process; role; user};***
	AU-06(07)	the permitted actions for each ***<AU-06(07)_ODP SELECTED PARAMETER VALUE(S)>*** associated with the review, analysis, and reporting of audit record information are specified.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-06(07)-Examine	[SELECT FROM: Audit and accountability policy; procedures addressing process, role and/or user permitted actions from audit review, analysis, and reporting; system security plan; privacy plan; other relevant documents or records].
	AU-06(07)-Interview	[SELECT FROM: Organizational personnel with audit review, analysis, and reporting responsibilities; organizational personnel with information security and privacy responsibilities].
	AU-06(07)-Test	[SELECT FROM: Mechanisms supporting permitted actions for the review, analysis, and reporting of audit information].

AU-06(08)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-06(08)	a full text analysis of logged privileged commands in a physically distinct component or subsystem of the system or other system that is dedicated to that analysis is performed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-06(08)-Examine	[SELECT FROM: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; system design documentation; system configuration settings and associated documentation; text analysis tools and techniques; text analysis documentation of audited privileged commands; system security plan; privacy plan; other relevant documents or records].
	AU-06(08)-Interview	[SELECT FROM: Organizational personnel with audit review, analysis, and reporting responsibilities; organizational personnel with information security and privacy responsibilities].
	AU-06(08)-Test	[SELECT FROM: Mechanisms implementing the capability to perform a full text analysis of audited privilege commands].

AU-06(09)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-06(09)	information from non-technical sources is correlated with audit record information to enhance organization-wide situational awareness.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-06(09)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing audit review, analysis, and reporting; system design documentation; system configuration settings and associated documentation; documentation providing evidence of correlated information obtained from audit records and organization-defined non-technical sources; list of information types from non-technical sources for correlation with audit information; other relevant documents or records].
	AU-06(09)-Interview	[SELECT FROM: Organizational personnel with audit review, analysis, and reporting responsibilities; organizational personnel with information security and privacy responsibilities].
	AU-06(09)-Test	[SELECT FROM: Mechanisms implementing capability to correlate information from non-technical sources].

AU-06(10)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | AUDIT LEVEL ADJUSTMENT
	[WITHDRAWN: Incorporated into AU-06.]

AU-07	AUDIT RECORD REDUCTION AND REPORT GENERATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-07a.[01]	an audit record reduction and report generation capability is provided that supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents;
	AU-07a.[02]	an audit record reduction and report generation capability is implemented that supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents;
	AU-07b.[01]	an audit record reduction and report generation capability is provided that does not alter the original content or time ordering of audit records;
	AU-07b.[02]	an audit record reduction and report generation capability is implemented that does not alter the original content or time ordering of audit records.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-07-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing audit reduction and report generation; system design documentation; system configuration settings and associated documentation; audit reduction, review, analysis, and reporting tools; system audit records; other relevant documents or records].

AU-07	AUDIT RECORD REDUCTION AND REPORT GENERATION	
	AU-07-Interview	[SELECT FROM: Organizational personnel with audit reduction and report generation responsibilities; organizational personnel with information security and privacy responsibilities].
	AU-07-Test	[SELECT FROM: Audit reduction and report generation capability].

AU-07(01)	AUDIT RECORD REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-07(01)_ODP	***fields within audit records that can be processed, sorted, or searched are defined;***
	AU-07(01)[01]	the capability to process, sort, and search audit records for events of interest based on ***<AU-07(01)_ODP fields within audit records>*** are provided;
	AU-07(01)[02]	the capability to process, sort, and search audit records for events of interest based on ***<AU-07(01)_ODP fields within audit records>*** are implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-07(01)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing audit reduction and report generation; system design documentation; system configuration settings and associated documentation; audit reduction, review, analysis, and reporting tools; audit record criteria (fields) establishing events of interest; system audit records; other relevant documents or records].
	AU-07(01)-Interview	[SELECT FROM: Organizational personnel with audit reduction and report generation responsibilities; organizational personnel with information security and privacy responsibilities; system developers].
	AU-07(01)-Test	[SELECT FROM: Audit reduction and report generation capability].

AU-07(02)	AUDIT RECORD REDUCTION AND REPORT GENERATION | AUTOMATIC SORT AND SEARCH
	[WITHDRAWN: Incorporated into AU-07(01).]

AU-08	TIME STAMPS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-08_ODP	***granularity of time measurement for audit record timestamps is defined;***
	AU-08a.	internal system clocks are used to generate timestamps for audit records;
	AU-08b.	timestamps are recorded for audit records that meet ***<AU-08_ODP granularity of time measurement>*** and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or include the local time offset as part of the timestamp.

AU-08	TIME STAMPS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-08-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing timestamp generation; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	AU-08-Interview	[SELECT FROM: Organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-08-Test	[SELECT FROM: Mechanisms implementing timestamp generation].

AU-08(01)	TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE
	[WITHDRAWN: Moved to SC-45(01).]

AU-08(02)	TIME STAMPS | SECONDARY AUTHORITATIVE TIME SOURCE
	[WITHDRAWN: Moved to SC-45(02).]

AU-09	PROTECTION OF AUDIT INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-09_ODP	***personnel or roles to be alerted upon detection of unauthorized access, modification, or deletion of audit information is/are defined;***
	AU-09a.	audit information and audit logging tools are protected from unauthorized access, modification, and deletion;
	AU-09b.	***<AU-09_ODP personnel or roles>*** are alerted upon detection of unauthorized access, modification, or deletion of audit information.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-09-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; access control policy and procedures; procedures addressing protection of audit information; system design documentation; system configuration settings and associated documentation; system audit records; audit tools; other relevant documents or records].
	AU-09-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-09-Test	[SELECT FROM: Mechanisms implementing audit information protection].

AU-09(01)	PROTECTION OF AUDIT INFORMATION | HARDWARE WRITE-ONCE MEDIA	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-09(01)	audit trails are written to hardware-enforced, write-once media.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-09(01)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; access control policy and procedures; procedures addressing protection of audit information; system design documentation; system hardware settings; system configuration settings and associated documentation; system storage media; system audit records; other relevant documents or records].
	AU-09(01)-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-09(01)-Test	[SELECT FROM: System media storing audit trails].

AU-09(02)	PROTECTION OF AUDIT INFORMATION | STORE ON SEPARATE PHYSICAL SYSTEMS OR COMPONENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-09(02)_ODP	***the frequency of storing audit records in a repository is defined;***
	AU-09(02)	audit records are stored ***<AU-09(02)_ODP frequency>*** in a repository that is part of a physically different system or system component than the system or component being audited.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-09(02)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing protection of audit information; system design documentation; system configuration settings and associated documentation; system or media storing backups of system audit records; system audit records; other relevant documents or records].
	AU-09(02)-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-09(02)-Test	[SELECT FROM: Mechanisms implementing the backing up of audit records].

AU-09(03)	PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-09(03)	cryptographic mechanisms to protect the integrity of audit information and audit tools are implemented.

AU-09(03)	PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-09(03)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; access control policy and procedures; procedures addressing protection of audit information; system design documentation; system hardware settings; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	AU-09(03)-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-09(03)-Test	[SELECT FROM: Cryptographic mechanisms protecting the integrity of audit information and tools].

AU-09(04)	PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-09(04)_ODP	***a subset of privileged users or roles authorized to access management of audit logging functionality is defined;***
	AU-09(04)	access to management of audit logging functionality is authorized only to ***<AU-09(04)_ODP subset of privileged users or roles>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-09(04)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; access control policy and procedures; procedures addressing protection of audit information; system design documentation; system configuration settings and associated documentation; system-generated list of privileged users with access to management of audit functionality; access authorizations; access control list; system audit records; other relevant documents or records].
	AU-09(04)-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	AU-09(04)-Test	[SELECT FROM: Mechanisms managing access to audit functionality].

AU-09(05)	PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-09(05)_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {movement; deletion};***
	AU-09(05)_ODP[02]	***audit information for which dual authorization is to be enforced is defined;***
	AU-09(05)	dual authorization is enforced for the ***<AU-09(05)_ODP[01] SELECTED PARAMETER VALUE(S)>*** of ***<AU-09(05)_ODP[02] audit information>***.

AU-09(05)	PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-09(05)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; access control policy and procedures; procedures addressing protection of audit information; system design documentation; system configuration settings and associated documentation; access authorizations; system audit records; other relevant documents or records].
	AU-09(05)-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	AU-09(05)-Test	[SELECT FROM: Mechanisms implementing the enforcement of dual authorization].

AU-09(06)	PROTECTION OF AUDIT INFORMATION | READ-ONLY ACCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-09(06)_ODP	***a subset of privileged users or roles with authorized read-only access to audit information is defined;***
	AU-09(06)	read-only access to audit information is authorized to ***<AU-09(06)_ODP subset of privileged users or roles>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-09(06)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; access control policy and procedures; procedures addressing protection of audit information; system design documentation; system configuration settings and associated documentation; system-generated list of privileged users with read-only access to audit information; access authorizations; access control list; system audit records; other relevant documents or records].
	AU-09(06)-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	AU-09(06)-Test	[SELECT FROM: Mechanisms managing access to audit information].

AU-09(07)	PROTECTION OF AUDIT INFORMATION | STORE ON COMPONENT WITH DIFFERENT OPERATING SYSTEM	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-09(07)	audit information is stored on a component running a different operating system than the system or component being audited.

AU-09(07)	PROTECTION OF AUDIT INFORMATION | STORE ON COMPONENT WITH DIFFERENT OPERATING SYSTEM	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-09(07)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; access control policy and procedures; procedures addressing protection of audit information; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	AU-09(07)-Interview	[SELECT FROM: Organizational personnel with audit and accountability responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	AU-09(07)-Test	[SELECT FROM: Mechanisms implementing operating system verification capability; mechanisms verifying audit information storage location].

AU-10	NON-REPUDIATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-10_ODP	***actions to be covered by non-repudiation are defined;***
	AU-10	irrefutable evidence is provided that an individual (or process acting on behalf of an individual) has performed ***<AU-10_ODP actions>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-10-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing non-repudiation; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	AU-10-Interview	[SELECT FROM: Organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-10-Test	[SELECT FROM: Mechanisms implementing non-repudiation capability].

AU-10(01)	NON-REPUDIATION | ASSOCIATION OF IDENTITIES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-10(01)_ODP	***the strength of binding between the identity of the information producer and the information is defined;***
	AU-10(01)(a)	the identity of the information producer is bound with the information to ***<AU-10(01)_ODP strength of binding>***;
	AU-10(01)(b)	the means for authorized individuals to determine the identity of the producer of the information is provided.

AU-10(01)	NON-REPUDIATION | ASSOCIATION OF IDENTITIES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-10(01)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing non-repudiation; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	AU-10(01)-Interview	[SELECT FROM: Organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-10(01)-Test	[SELECT FROM: Mechanisms implementing non-repudiation capability].

AU-10(02)	NON-REPUDIATION | VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-10(02)_ODP[01]	***the frequency at which to validate the binding of the information producer identity to the information is defined;***
	AU-10(02)_ODP[02]	***the actions to be performed in the event of a validation error are defined;***
	AU-10(02)(a)	the binding of the information producer identity to the information is validated at ***<AU-10(02)_ODP[01] frequency>***;
	AU-10(02)(b)	***<AU-10(02)_ODP[02] actions>*** in the event of a validation error are performed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-10(02)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing non-repudiation; system design documentation; system configuration settings and associated documentation; validation records; system audit records; other relevant documents or records].
	AU-10(02)-Interview	[SELECT FROM: Organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-10(02)-Test	[SELECT FROM: Mechanisms implementing non-repudiation capability].

AU-10(03)	NON-REPUDIATION | CHAIN OF CUSTODY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-10(03)	reviewer or releaser credentials are maintained within the established chain of custody for information reviewed or released.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-10(03)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing non-repudiation; system design documentation; system configuration settings and associated documentation; records of information reviews and releases; system audit records; other relevant documents or records].

AU-10(03)	NON-REPUDIATION | CHAIN OF CUSTODY	
	AU-10(03)-Interview	[SELECT FROM: Organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-10(03)-Test	[SELECT FROM: Automated mechanisms implementing non-repudiation capability].

AU-10(04)	NON-REPUDIATION | VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-10(04)_ODP[01]	***security domains for which the binding of the information reviewer identity to the information is to be validated at transfer or release are defined;***
	AU-10(04)_ODP[02]	***actions to be performed in the event of a validation error are defined;***
	AU-10(04)(a)	the binding of the information reviewer identity to the information at the transfer or release points prior to release or transfer between ***<AU-10(04)_ODP[01] security domains>*** is validated;
	AU-10(04)(b)	***<AU-10(04)_ODP[02] actions>*** are performed in the event of a validation error.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-10(04)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing non-repudiation; system design documentation; system configuration settings and associated documentation; validation records; system audit records; other relevant documents or records].
	AU-10(04)-Interview	[SELECT FROM: Organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-10(04)-Test	[SELECT FROM: Mechanisms implementing non-repudiation capability].

AU-10(05)	NON-REPUDIATION | DIGITAL SIGNATURES
	[WITHDRAWN: Incorporated into SI-07.]

AU-11	AUDIT RECORD RETENTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-11_ODP	***a time period to retain audit records that is consistent with the records retention policy is defined;***
	AU-11	audit records are retained for ***<AU-11_ODP time period>*** to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

AU-11	AUDIT RECORD RETENTION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-11-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; audit record retention policy and procedures; security plan; organization-defined retention period for audit records; audit record archives; audit logs; audit records; other relevant documents or records].
	AU-11-Interview	[SELECT FROM: Organizational personnel with audit record retention responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].

AU-11(01)	AUDIT RECORD RETENTION | LONG-TERM RETRIEVAL CAPABILITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-11(01)_ODP	***measures to be employed to ensure that long-term audit records generated by the system can be retrieved are defined;***
	AU-11(01)	***<AU-11(01)_ODP measures>*** are employed to ensure that long-term audit records generated by the system can be retrieved.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-11(01)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; audit record retention policy and procedures; system design documentation; system configuration settings and associated documentation; audit record archives; audit logs; audit records; other relevant documents or records].
	AU-11(01)-Interview	[SELECT FROM: Organizational personnel with audit record retention responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	AU-11(01)-Test	[SELECT FROM: Mechanisms implementing audit record retention capability].

AU-12	AUDIT RECORD GENERATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-12_ODP[01]	***system components that provide an audit record generation capability for the events types (defined in AU-02_ODP[02]) are defined;***
	AU-12_ODP[02]	***personnel or roles allowed to select the event types that are to be logged by specific components of the system is/are defined;***
	AU-12a.	audit record generation capability for the event types the system is capable of auditing (defined in AU-02_ODP[01]) is provided by ***<AU-12_ODP[01] system components>***;
	AU-12b.	***<AU-12_ODP[02] personnel or roles>*** is/are allowed to select the event types that are to be logged by specific components of the system;
	AU-12c.	audit records for the event types defined in AU-02_ODP[02] that include the audit record content defined in AU-03 are generated.

AU-12	AUDIT RECORD GENERATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-12-Examine	[SELECT FROM: Audit and accountability policy; procedures addressing audit record generation; system security plan; privacy plan; system design documentation; system configuration settings and associated documentation; list of auditable events; system audit records; other relevant documents or records].
	AU-12-Interview	[SELECT FROM: Organizational personnel with audit record generation responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-12-Test	[SELECT FROM: Mechanisms implementing audit record generation capability].

AU-12(01)	AUDIT RECORD GENERATION | SYSTEM-WIDE AND TIME-CORRELATED AUDIT TRAIL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-12(01)_ODP[01]	***system components from which audit records are to be compiled into a system-wide (logical or physical) audit trail are defined;***
	AU-12(01)_ODP[02]	***level of tolerance for the relationship between timestamps of individual records in the audit trail is defined;***
	AU-12(01)	audit records from ***<AU-12(01)_ODP[01] system components>*** are compiled into a system-wide (logical or physical) audit trail that is time-correlated to within ***<AU-12(01)_ODP[02] level of tolerance>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-12(01)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing audit record generation; system design documentation; system configuration settings and associated documentation; system-wide audit trail (logical or physical); system audit records; other relevant documents or records].
	AU-12(01)-Interview	[SELECT FROM: Organizational personnel with audit record generation responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-12(01)-Test	[SELECT FROM: Mechanisms implementing audit record generation capability].

AU-12(02)	AUDIT RECORD GENERATION | STANDARDIZED FORMATS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-12(02)	a system-wide (logical or physical) audit trail composed of audit records is produced in a standardized format.

AU-12(02)	AUDIT RECORD GENERATION | STANDARDIZED FORMATS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-12(02)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing audit record generation; system design documentation; system configuration settings and associated documentation; system-wide audit trail (logical or physical); system audit records; other relevant documents or records].
	AU-12(02)-Interview	[SELECT FROM: Organizational personnel with audit record generation responsibilities; organizational personnel with security responsibilities; system/network administrators; system developers].
	AU-12(02)-Test	[SELECT FROM: Mechanisms implementing audit record generation capability].

AU-12(03)	AUDIT RECORD GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-12(03)_ODP[01]	***individuals or roles authorized to change the logging on system components are defined;***
	AU-12(03)_ODP[02]	***system components on which logging is to be performed are defined;***
	AU-12(03)_ODP[03]	***selectable event criteria with which change logging is to be performed are defined;***
	AU-12(03)_ODP[04]	***time thresholds in which logging actions are to change is defined;***
	AU-12(03)[01]	the capability for ***<AU-12(03)_ODP[01] individuals or roles>*** to change the logging to be performed on ***<AU-12(03)_ODP[02] system components>*** based on ***<AU-12(03)_ODP[03] selectable event criteria>*** within ***<AU-12(03)_ODP[04] time thresholds>*** is provided;
	AU-12(03)[02]	the capability for ***<AU-12(03)_ODP[01] individuals or roles>*** to change the logging to be performed on ***<AU-12(03)_ODP[02] system components>*** based on ***<AU-12(03)_ODP[03] selectable event criteria>*** within ***<AU-12(03)_ODP[04] time thresholds>*** is implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-12(03)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing audit record generation; system design documentation; system configuration settings and associated documentation; system-generated list of individuals or roles authorized to change auditing to be performed; system audit records; other relevant documents or records].
	AU-12(03)-Interview	[SELECT FROM: Organizational personnel with audit record generation responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-12(03)-Test	[SELECT FROM: Mechanisms implementing audit record generation capability].

AU-12(04)	AUDIT RECORD GENERATION | QUERY PARAMETER AUDITS OF PERSONALLY IDENTIFIABLE INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-12(04)[01]	the capability to audit the parameters of user query events for data sets containing personally identifiable information is provided;
	AU-12(04)[02]	the capability to audit the parameters of user query events for data sets containing personally identifiable information is implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-12(04)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing audit record generation; query event records; system design documentation; system configuration settings and associated documentation; map of system data actions; system audit records; other relevant documents or records].
	AU-12(04)-Interview	[SELECT FROM: Organizational personnel with audit record generation responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-12(04)-Test	[SELECT FROM: Mechanisms implementing audit record generation capability].

AU-13	MONITORING FOR INFORMATION DISCLOSURE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-13_ODP[01]	***open-source information and/or information sites to be monitored for evidence of unauthorized disclosure of organizational information is/are defined;***
	AU-13_ODP[02]	***the frequency with which open-source information and/or information sites are monitored for evidence of unauthorized disclosure of organizational information is defined;***
	AU-13_ODP[03]	***personnel or roles to be notified if an information disclosure is discovered is/are defined;***
	AU-13_ODP[04]	***additional actions to be taken if an information disclosure is discovered are defined;***
	AU-13a.	***<AU-13_ODP[01] open-source information and/or information sites>*** is/are monitored ***<AU-13_ODP[02] frequency>*** for evidence of unauthorized disclosure of organizational information;
	AU-13b.01	***<AU-13_ODP[03] personnel or roles>*** are notified if an information disclosure is discovered;
	AU-13b.02	***<AU-13_ODP[04] additional actions>*** are taken if an information disclosure is discovered.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-13-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing information disclosure monitoring; system design documentation; system configuration settings and associated documentation; monitoring records; system audit records; other relevant documents or records].

AU-13	MONITORING FOR INFORMATION DISCLOSURE	
	AU-13-Interview	[SELECT FROM: Organizational personnel with responsibilities for monitoring open-source information and/or information sites; organizational personnel with security and privacy responsibilities].
	AU-13-Test	[SELECT FROM: Mechanisms implementing monitoring for information disclosure].

AU-13(01)	MONITORING FOR INFORMATION DISCLOSURE | USE OF AUTOMATED TOOLS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-13(01)_ODP	***automated mechanisms for monitoring open-source information and information sites are defined;***
	AU-13(01)	open-source information and information sites are monitored using ***<AU-13(01)_ODP automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-13(01)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing information disclosure monitoring; system design documentation; system configuration settings and associated documentation; automated monitoring tools; system audit records; other relevant documents or records].
	AU-13(01)-Interview	[SELECT FROM: Organizational personnel with responsibilities for monitoring information disclosures; organizational personnel with information security and privacy responsibilities].
	AU-13(01)-Test	[SELECT FROM: Automated mechanisms implementing monitoring for information disclosure].

AU-13(02)	MONITORING FOR INFORMATION DISCLOSURE | REVIEW OF MONITORED SITES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-13(02)_ODP	***the frequency at which to review the open-source information sites being monitored is defined;***
	AU-13(02)	the list of open-source information sites being monitored is reviewed ***<AU-13(02)_ODP frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-13(02)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing information disclosure monitoring; system design documentation; system configuration settings and associated documentation; reviews for open-source information sites being monitored; system audit records; other relevant documents or records].
	AU-13(02)-Interview	[SELECT FROM: Organizational personnel with responsibilities for monitoring open-source information sites; organizational personnel with information security and privacy responsibilities].

AU-13(02)	MONITORING FOR INFORMATION DISCLOSURE | REVIEW OF MONITORED SITES	
	AU-13(02)-Test	[SELECT FROM: Mechanisms implementing monitoring for information disclosure].

AU-13(03)	MONITORING FOR INFORMATION DISCLOSURE | UNAUTHORIZED REPLICATION OF INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-13(03)	discovery techniques, processes, and tools are employed to determine if external entities are replicating organizational information in an unauthorized manner.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-13(03)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing information disclosure monitoring; procedures addressing information replication; system design documentation; system configuration settings and associated documentation; system audit records; training resources for staff to recognize the unauthorized use of organizational information; other relevant documents or records].
	AU-13(03)-Interview	[SELECT FROM: Organizational personnel with responsibilities for monitoring unauthorized replication of information; organizational personnel with information security and privacy responsibilities].
	AU-13(03)-Test	[SELECT FROM: Discovery tools for identifying unauthorized information replication].

AU-14	SESSION AUDIT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-14_ODP[01]	***users or roles who can audit the content of a user session are defined;***
	AU-14_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {record; view; hear; log};***
	AU-14_ODP[03]	***circumstances under which the content of a user session can be audited are defined;***
	AU-14a.[01]	***<AU-14_ODP[01] users or roles>*** are provided with the capability to ***<AU-14_ODP[02] SELECTED PARAMETER VALUE(S)>*** the content of a user session under ***<AU-14_ODP[03] circumstances>***;
	AU-14a.[02]	the capability for ***<AU-14_ODP[01] users or roles>*** to ***<AU-14_ODP[02] SELECTED PARAMETER VALUE(S)>*** the content of a user session under ***<AU-14_ODP[03] circumstances>*** is implemented;
	AU-14b.[01]	session auditing activities are developed in consultation with legal counsel and in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines;

AU-14	SESSION AUDIT	
	AU-14b.[02]	session auditing activities are integrated in consultation with legal counsel and in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines;
	AU-14b.[03]	session auditing activities are used in consultation with legal counsel and in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines;
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-14-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing user session auditing; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	AU-14-Interview	[SELECT FROM: Organizational personnel with information security and privacy responsibilities; system/network administrators; system developers; legal counsel; personnel with civil liberties responsibilities].
	AU-14-Test	[SELECT FROM: Mechanisms implementing user session auditing capability].

AU-14(01)	SESSION AUDIT | SYSTEM START-UP	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-14(01)	session audits are initiated automatically at system start-up.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-14(01)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing user session auditing; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	AU-14(01)-Interview	[SELECT FROM: Organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	AU-14(01)-Test	[SELECT FROM: Mechanisms implementing user session auditing capability].

AU-14(02)	SESSION AUDIT | CAPTURE AND RECORD CONTENT
	[WITHDRAWN: Incorporated into AU-14.]

AU-14(03)	SESSION AUDIT | REMOTE VIEWING AND LISTENING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-14(03)[01]	the capability for authorized users to remotely view and hear content related to an established user session in real time is provided;

AU-14(03)	SESSION AUDIT | REMOTE VIEWING AND LISTENING	
	AU-14(03)[02]	the capability for authorized users to remotely view and hear content related to an established user session in real time is implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-14(03)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing user session auditing; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	AU-14(03)-Interview	[SELECT FROM: Organizational personnel with information security and privacy responsibilities; system/network administrators; system developers; legal counsel; personnel with civil liberties responsibilities].
	AU-14(03)-Test	[SELECT FROM: Mechanisms implementing user session auditing capability].

AU-15	ALTERNATE AUDIT LOGGING CAPABILITY
	[WITHDRAWN: Moved to AU-05(05).]

AU-16	CROSS-ORGANIZATIONAL AUDIT LOGGING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-16_ODP[01]	***methods for coordinating audit information among external organizations when audit information is transmitted across organizational boundaries are defined;***
	AU-16_ODP[02]	***audit information to be coordinated among external organizations when audit information is transmitted across organizational boundaries is defined;***
	AU-16	***<AU-16_ODP[01] methods>*** for coordinating ***<AU-16_ODP[02] audit information>*** among external organizations when audit information is transmitted across organizational boundaries are employed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-16-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing methods for coordinating audit information among external organizations; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	AU-16-Interview	[SELECT FROM: Organizational personnel with responsibilities for coordinating audit information among external organizations; organizational personnel with information security and privacy responsibilities].
	AU-16-Test	[SELECT FROM: Mechanisms implementing cross-organizational auditing].

AU-16(01)	CROSS-ORGANIZATIONAL AUDIT LOGGING | IDENTITY PRESERVATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-16(01)	the identity of individuals in cross-organizational audit trails is preserved.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-16(01)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing cross-organizational audit trails; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	AU-16(01)-Interview	[SELECT FROM: Organizational personnel with cross-organizational audit responsibilities; organizational personnel with information security and privacy responsibilities].
	AU-16(01)-Test	[SELECT FROM: Mechanisms implementing cross-organizational auditing (if applicable)].

AU-16(02)	CROSS-ORGANIZATIONAL AUDIT LOGGING | SHARING OF AUDIT INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-16(02)_ODP[01]	***organizations with which cross-organizational audit information is to be shared are defined;***
	AU-16(02)_ODP[02]	***cross-organizational sharing agreements to be used when providing cross-organizational audit information to organizations are defined;***
	AU-16(02)	cross-organizational audit information is provided to ***<AU-16(02)_ODP[01] organizations>*** based on ***<AU-16(02)_ODP[02] cross-organizational sharing agreements>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-16(02)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing cross-organizational sharing of audit information; information sharing agreements; other relevant documents or records].
	AU-16(02)-Interview	[SELECT FROM: Organizational personnel with responsibilities for sharing cross-organizational audit information; organizational personnel with information security and privacy responsibilities].

AU-16(03)	CROSS-ORGANIZATIONAL AUDIT LOGGING | DISASSOCIABILITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	AU-16(03)_ODP	***measures to disassociate individuals from audit information transmitted across organizational boundaries are defined;***
	AU-16(03)	***<AU-16(03)_ODP measures>*** are implemented to disassociate individuals from audit information transmitted across organizational boundaries.

AU-16(03)	CROSS-ORGANIZATIONAL AUDIT LOGGING | DISASSOCIABILITY	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AU-16(03)-Examine	[SELECT FROM: Audit and accountability policy; system security plan; privacy plan; procedures addressing cross-organizational sharing of audit information; policy and/or procedures regarding the deidentification of PII; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	AU-16(03)-Interview	[SELECT FROM: Organizational personnel with responsibilities for sharing cross-organizational audit information; organizational personnel with information security and privacy responsibilities].
	AU-16(03)-Test	[SELECT FROM: Mechanisms implementing disassociability].

4.4 ASSESSMENT, AUTHORIZATION, AND MONITORING

CA-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-01_ODP[01]	***personnel or roles to whom the assessment, authorization, and monitoring policy is to be disseminated is/are defined;***
	CA-01_ODP[02]	***personnel or roles to whom the assessment, authorization, and monitoring procedures are to be disseminated is/are defined;***
	CA-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	CA-01_ODP[04]	***an official to manage the assessment, authorization, and monitoring policy and procedures is defined;***
	CA-01_ODP[05]	***the frequency at which the current assessment, authorization, and monitoring policy is reviewed and updated is defined;***
	CA-01_ODP[06]	***events that would require the current assessment, authorization, and monitoring policy to be reviewed and updated are defined;***
	CA-01_ODP[07]	***the frequency at which the current assessment, authorization, and monitoring procedures are reviewed and updated is defined;***
	CA-01_ODP[08]	***events that would require assessment, authorization, and monitoring procedures to be reviewed and updated are defined;***
	CA-01a.[01]	an assessment, authorization, and monitoring policy is developed and documented;
	CA-01a.[02]	the assessment, authorization, and monitoring policy is disseminated to ***<CA-01_ODP[01] personnel or roles>***;
	CA-01a.[03]	assessment, authorization, and monitoring procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and associated assessment, authorization, and monitoring controls are developed and documented;
	CA-01a.[04]	the assessment, authorization, and monitoring procedures are disseminated to ***<CA-01_ODP[02] personnel or roles>***;
	CA-01a.01(a)[01]	the ***<CA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** assessment, authorization, and monitoring policy addresses purpose;
	CA-01a.01(a)[02]	the ***<CA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** assessment, authorization, and monitoring policy addresses scope;[03] SELECTED PARAMETER(S)> assessment, authorization, and monitoring policy addresses scope;
	CA-01a.01(a)[03]	the ***<CA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** assessment, authorization, and monitoring policy addresses roles;[03] SELECTED PARAMETER(S)> assessment, authorization, and monitoring policy addresses roles;
	CA-01a.01(a)[04]	the ***<CA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** assessment, authorization, and monitoring policy addresses responsibilities;
	CA-01a.01(a)[05]	the ***<CA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** assessment, authorization, and monitoring policy addresses management commitment;

CA-01	POLICY AND PROCEDURES	
	CA-01a.01(a)[06]	the ***<CA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** assessment, authorization, and monitoring policy addresses coordination among organizational entities;
	CA-01a.01(a)[07]	the ***<CA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** assessment, authorization, and monitoring policy addresses compliance;
	CA-01a.01(b)	the ***<CA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** assessment, authorization, and monitoring policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines;
	CA-01b.	the ***<CA-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures;
	CA-01c.01[01]	the current assessment, authorization, and monitoring policy is reviewed and updated ***<CA-01_ODP[05] frequency>***;
	CA-01c.01[02]	the current assessment, authorization, and monitoring policy is reviewed and updated following ***<CA-01_ODP[06] events>***;
	CA-01c.02[01]	the current assessment, authorization, and monitoring procedures are reviewed and updated ***<CA-01_ODP[07] frequency>***;
	CA-01c.02[02]	the current assessment, authorization, and monitoring procedures are reviewed and updated following ***<CA-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-01-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy and procedures; system security plan; privacy plan; other relevant documents or records].
	CA-01-Interview	[SELECT FROM: Organizational personnel with assessment, authorization, and monitoring policy responsibilities; organizational personnel with information security and privacy responsibilities].

CA-02	CONTROL ASSESSMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-02_ODP[01]	***the frequency at which to assess controls in the system and its environment of operation is defined;***
	CA-02_ODP[02]	***individuals or roles to whom control assessment results are to be provided are defined;***
	CA-02a.	an appropriate assessor or assessment team is selected for the type of assessment to be conducted;
	CA-02b.01	a control assessment plan is developed that describes the scope of the assessment, including controls and control enhancements under assessment;
	CA-02b.02	a control assessment plan is developed that describes the scope of the assessment, including assessment procedures to be used to determine control effectiveness;
	CA-02b.03[01]	a control assessment plan is developed that describes the scope of the assessment, including the assessment environment;

CA-02	CONTROL ASSESSMENTS	
	CA-02b.03[02]	a control assessment plan is developed that describes the scope of the assessment, including the assessment team;
	CA-02b.03[03]	a control assessment plan is developed that describes the scope of the assessment, including assessment roles and responsibilities;
	CA-02c.	the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
	CA-02d.[01]	controls are assessed in the system and its environment of operation ***<CA-02_ODP[01] assessment frequency>*** to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
	CA-02d.[02]	controls are assessed in the system and its environment of operation ***<CA-02_ODP[01] assessment frequency>*** to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established privacy requirements;
	CA-02e.	a control assessment report is produced that documents the results of the assessment;
	CA-02f.	the results of the control assessment are provided to ***<CA-02_ODP[02] individuals or roles>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-02-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; procedures addressing assessment planning; procedures addressing control assessments; control assessment plan; control assessment report; system security plan; privacy plan; other relevant documents or records].
	CA-02-Interview	[SELECT FROM: Organizational personnel with control assessment responsibilities; organizational personnel with information security and privacy responsibilities].
	CA-02-Test	[SELECT FROM: Mechanisms supporting control assessment, control assessment plan development, and/or control assessment reporting].

CA-02(01)	CONTROL ASSESSMENTS | INDEPENDENT ASSESSORS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-02(01)	independent assessors or assessment teams are employed to conduct control assessments.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-02(01)-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; procedures addressing control assessments; previous control assessment plan; previous control assessment report; plan of action and milestones; existing authorization statement; system security plan; privacy plan; other relevant documents or records].
	CA-02(01)-Interview	[SELECT FROM: Organizational personnel with security assessment responsibilities; organizational personnel with information security and privacy responsibilities].

CA-02(02)	CONTROL ASSESSMENTS | SPECIALIZED ASSESSMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-02(02)_ODP[01]	***frequency at which to include specialized assessments as part of the control assessment is defined;***
	CA-02(02)_ODP[02]	***one of the following PARAMETER VALUES is selected: {announced; unannounced};***
	CA-02(02)_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {in-depth monitoring; security instrumentation; automated security test cases; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; data leakage or data loss assessment; <CA-02(02)_ODP[04] other forms of assessment>};***
	CA-02(02)_ODP[04]	***other forms of assessment are defined (if selected);***
	CA-02(02)	***<CA-02(02)_ODP[01] specialized assessment frequency> <CA-02(02)_ODP[02] SELECTED PARAMETER VALUE> <CA-02(02)_ODP[03] SELECTED PARAMETER VALUE(S)>*** are included as part of control assessments.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-02(02)-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; procedures addressing control assessments; control assessment plan; control assessment report; control assessment evidence; system security plan; privacy plan; other relevant documents or records].
	CA-02(02)-Interview	[SELECT FROM: Organizational personnel with control assessment responsibilities; organizational personnel with information security and privacy responsibilities].
	CA-02(02)-Test	[SELECT FROM: Mechanisms supporting control assessment].

CA-02(03)	CONTROL ASSESSMENTS | LEVERAGING RESULTS FROM EXTERNAL ORGANIZATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-02(03)_ODP[01]	***external organizations from which the results of control assessments are leveraged are defined;***
	CA-02(03)_ODP[02]	***system on which a control assessment was performed by an external organization is defined;***
	CA-02(03)_ODP[03]	***requirements to be met by the control assessment performed by an external organization on the system are defined;***
	CA-02(03)	the results of control assessments performed by ***<CA-02(03)_ODP[01] external organizations>*** on ***<CA-02(03)_ODP[02] system>*** are leveraged when the assessment meets ***<CA-02(03)_ODP[03] requirements>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-02(03)-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; procedures addressing control assessments; control assessment requirements; control assessment plan; control assessment report; control assessment evidence; plan of action and milestones; system security plan; privacy plan; other relevant documents or records].

CA-02(03)	CONTROL ASSESSMENTS | LEVERAGING RESULTS FROM EXTERNAL ORGANIZATIONS	
	CA-02(03)-Interview	[SELECT FROM: Organizational personnel with control assessment responsibilities; organizational personnel with information security and privacy responsibilities; personnel performing control assessments for the specified external organization].

CA-03	INFORMATION EXCHANGE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-03_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; non-disclosure agreements; <CA-03_ODP[02] type of agreement>};***
	CA-03_ODP[02]	***the type of agreement used to approve and manage the exchange of information is defined (if selected);***
	CA-03_ODP[03]	***the frequency at which to review and update agreements is defined;***
	CA-03a.	the exchange of information between the system and other systems is approved and managed using ***<CA-03_ODP[01] SELECTED PARAMETER VALUE(S)>***;
	CA-03b.[01]	the interface characteristics are documented as part of each exchange agreement;
	CA-03b.[02]	security requirements are documented as part of each exchange agreement;
	CA-03b.[03]	privacy requirements are documented as part of each exchange agreement;
	CA-03b.[04]	controls are documented as part of each exchange agreement;
	CA-03b.[05]	responsibilities for each system are documented as part of each exchange agreement;
	CA-03b.[06]	the impact level of the information communicated is documented as part of each exchange agreement;
	CA-03c.	agreements are reviewed and updated ***<CA-03_ODP[03] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-03-Examine	[SELECT FROM: Access control policy; procedures addressing system connections; system and communications protection policy; system interconnection security agreements; information exchange security agreements; memoranda of understanding or agreements; service level agreements; non-disclosure agreements; system design documentation; enterprise architecture; system architecture; system configuration settings and associated documentation; system security plan; privacy plan; other relevant documents or records].
	CA-03-Interview	[SELECT FROM: Organizational personnel with responsibilities for developing, implementing, or approving system interconnection agreements; organizational personnel with information security and privacy responsibilities; personnel managing the system(s) to which the interconnection security agreement applies].

CA-03(01)	INFORMATION EXCHANGE | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS
	[WITHDRAWN: Moved to SC-07(25).]

CA-03(02)	INFORMATION EXCHANGE | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS
	[WITHDRAWN: Moved to SC-07(26).]

CA-03(03)	INFORMATION EXCHANGE | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS
	[WITHDRAWN: Moved to SC-07(27).]

CA-03(04)	INFORMATION EXCHANGE | CONNECTIONS TO PUBLIC NETWORKS
	[WITHDRAWN: Moved to SC-07(28).]

CA-03(05)	INFORMATION EXCHANGE | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS
	[WITHDRAWN: Moved to SC-07(05).]

CA-03(06)	INFORMATION EXCHANGE | TRANSFER AUTHORIZATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-03(06)	individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-03(06)-Examine	[SELECT FROM: Access control policy; procedures addressing system connections; system and communications protection policy; system interconnection agreements; information exchange security agreements; memoranda of understanding or agreements; service level agreements; non-disclosure agreements; system design documentation; system configuration settings and associated documentation; control assessment report; system audit records; system security plan; privacy plan; other relevant documents or records].
	CA-03(06)-Interview	[SELECT FROM: Organizational personnel with responsibilities for managing connections to external systems; network administrators; organizational personnel with information security and privacy responsibilities].
	CA-03(06)-Test	[SELECT FROM: Mechanisms implementing restrictions on external system connections].

CA-03(07)	INFORMATION EXCHANGE | TRANSITIVE INFORMATION EXCHANGES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-03(07)(a)	transitive (downstream) information exchanges with other systems through the systems identified in CA-03a are identified;
	CA-03(07)(b)	measures are taken to ensure that transitive (downstream) information exchanges cease when the controls on identified transitive (downstream) systems cannot be verified or validated.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-03(07)-Examine	[SELECT FROM: Access control policy; procedures addressing system connections; system and communications protection policy; system interconnection agreements; information exchange security agreements; memoranda of understanding or agreements; service level agreements; non-disclosure agreements; system design documentation; system configuration settings and associated documentation; control assessment report; system audit records; system security plan; privacy plan; other relevant documents or records].
	CA-03(07)-Interview	[SELECT FROM: Organizational personnel with responsibilities for managing connections to external systems; network administrators; organizational personnel with information security and privacy responsibilities].
	CA-03(07)-Test	[SELECT FROM: Mechanisms implementing restrictions on external system connections].

CA-04	SECURITY CERTIFICATION
	[WITHDRAWN: Incorporated into CA-02.]

CA-05	PLAN OF ACTION AND MILESTONES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-05_ODP	***the frequency at which to update an existing plan of action and milestones based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities is defined;***
	CA-05a.	a plan of action and milestones for the system is developed to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system;
	CA-05b.	existing plan of action and milestones are updated ***<CA-05_ODP frequency>*** based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

CA-05	PLAN OF ACTION AND MILESTONES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-05-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; procedures addressing plan of action and milestones; control assessment plan; control assessment report; control assessment evidence; plan of action and milestones; system security plan; privacy plan; other relevant documents or records].
	CA-05-Interview	[SELECT FROM: Organizational personnel with plan of action and milestones development and implementation responsibilities; organizational personnel with information security and privacy responsibilities].
	CA-05-Test	[SELECT FROM: Mechanisms for developing, implementing, and maintaining plan of action and milestones].

CA-05(01)	PLAN OF ACTION AND MILESTONES | AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-05(01)_ODP	***automated mechanisms used to ensure the accuracy, currency, and availability of the plan of action and milestones for the system are defined;***
	CA-05(01)	***<CA-05(01)_ODP automated mechanisms>*** are used to ensure the accuracy, currency, and availability of the plan of action and milestones for the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-05(01)-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; procedures addressing plan of action and milestones; system design documentation; system configuration settings and associated documentation; system audit records; plan of action and milestones; system security plan; privacy plan; other relevant documents or records].
	CA-05(01)-Interview	[SELECT FROM: Organizational personnel with plan of action and milestones development and implementation responsibilities; organizational personnel with information security and privacy responsibilities].
	CA-05(01)-Test	[SELECT FROM: Automated mechanisms for developing, implementing, and maintaining a plan of action and milestones].

CA-06	AUTHORIZATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-06_ODP	***frequency at which to update the authorizations is defined;***
	CA-06a.	a senior official is assigned as the authorizing official for the system;
	CA-06b.	a senior official is assigned as the authorizing official for common controls available for inheritance by organizational systems;

CA-06	AUTHORIZATION	
	CA-06c.01	before commencing operations, the authorizing official for the system accepts the use of common controls inherited by the system;
	CA-06c.02	before commencing operations, the authorizing official for the system authorizes the system to operate;
	CA-06d.	the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;
	CA-06e.	the authorizations are updated ***<CA-06_ODP frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-06-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; procedures addressing authorization; system security plan, privacy plan, assessment report, plan of action and milestones; authorization statement; other relevant documents or records].
	CA-06-Interview	[SELECT FROM: Organizational personnel with authorization responsibilities; organizational personnel with information security and privacy responsibilities].
	CA-06-Test	[SELECT FROM: Mechanisms that facilitate authorizations and updates].

CA-06(01)	AUTHORIZATION | JOINT AUTHORIZATION — INTRA-ORGANIZATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-06(01)[01]	a joint authorization process is employed for the system;
	CA-06(01)[02]	the joint authorization process employed for the system includes multiple authorizing officials from the same organization conducting the authorization.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-06(01)-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; procedures addressing authorization; system security plan; privacy plan; assessment report; plan of action and milestones; authorization statement; other relevant documents or records].
	CA-06(01)-Interview	[SELECT FROM: Organizational personnel with authorization responsibilities; organizational personnel with information security and privacy responsibilities].
	CA-06(01)-Test	[SELECT FROM: Mechanisms that facilitate authorizations and updates].

CA-06(02)	AUTHORIZATION | JOINT AUTHORIZATION — INTER-ORGANIZATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-06(02)[01]	a joint authorization process is employed for the system;
	CA-06(02)[02]	the joint authorization process employed for the system includes multiple authorizing officials with at least one authorizing official from an organization external to the organization conducting the authorization.

CA-06(02)	AUTHORIZATION | JOINT AUTHORIZATION — INTER-ORGANIZATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-06(02)-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; procedures addressing authorization; system security plan; privacy plan; assessment report; plan of action and milestones; authorization statement; other relevant documents or records].
	CA-06(02)-Interview	[SELECT FROM: Organizational personnel with authorization responsibilities; organizational personnel with information security and privacy responsibilities].
	CA-06(02)-Test	[SELECT FROM: Mechanisms that facilitate authorizations and updates].

CA-07	CONTINUOUS MONITORING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-07_ODP[01]	***system-level metrics to be monitored are defined;***
	CA-07_ODP[02]	***frequencies at which to monitor control effectiveness are defined;***
	CA-07_ODP[03]	***frequencies at which to assess control effectiveness are defined;***
	CA-07_ODP[04]	***personnel or roles to whom the security status of the system is reported are defined;***
	CA-07_ODP[05]	***frequency at which the security status of the system is reported is defined;***
	CA-07_ODP[06]	***personnel or roles to whom the privacy status of the system is reported are defined;***
	CA-07_ODP[07]	***frequency at which the privacy status of the system is reported is defined;***
	CA-07[01]	a system-level continuous monitoring strategy is developed;
	CA-07[02]	system-level continuous monitoring is implemented in accordance with the organization-level continuous monitoring strategy;
	CA-07a.	system-level continuous monitoring includes establishment of the following system-level metrics to be monitored: ***<CA-07_ODP[01] system-level metrics>***;
	CA-07b.[01]	system-level continuous monitoring includes established ***<CA-07_ODP[02] frequencies>*** for monitoring;
	CA-07b.[02]	system-level continuous monitoring includes established ***<CA-07_ODP[03] frequencies>*** for assessment of control effectiveness;
	CA-07c.	system-level continuous monitoring includes ongoing control assessments in accordance with the continuous monitoring strategy;
	CA-07d.	system-level continuous monitoring includes ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
	CA-07e.	system-level continuous monitoring includes correlation and analysis of information generated by control assessments and monitoring;
	CA-07f.	system-level continuous monitoring includes response actions to address the results of the analysis of control assessment and monitoring information;

CA-07	CONTINUOUS MONITORING	
	CA-07g.[01]	system-level continuous monitoring includes reporting the security status of the system to ***<CA-07_ODP[04] personnel or roles> <CA-07_ODP[05] frequency>***;
	CA-07g.[02]	system-level continuous monitoring includes reporting the privacy status of the system to ***<CA-07_ODP[06] personnel or roles> <CA-07_ODP[07] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-07-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; organizational continuous monitoring strategy; system-level continuous monitoring strategy; procedures addressing continuous monitoring of system controls; procedures addressing configuration management; control assessment report; plan of action and milestones; system monitoring records; configuration management records; impact analyses; status reports; system security plan; privacy plan; other relevant documents or records].
	CA-07-Interview	[SELECT FROM: Organizational personnel with continuous monitoring responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	CA-07-Test	[SELECT FROM: Mechanisms implementing continuous monitoring; mechanisms supporting response actions to address assessment and monitoring results; mechanisms supporting security and privacy status reporting].

CA-07(01)	CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-07(01)	independent assessors or assessment teams are employed to monitor the controls in the system on an ongoing basis.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-07(01)-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; organizational continuous monitoring strategy; system-level continuous monitoring strategy; procedures addressing continuous monitoring of system controls; control assessment report; plan of action and milestones; system monitoring records; impact analyses; status reports; system security plan; privacy plan; other relevant documents or records].
	CA-07(01)-Interview	[SELECT FROM: Organizational personnel with continuous monitoring responsibilities; organizational personnel with information security and privacy responsibilities].

CA-07(02)	CONTINUOUS MONITORING | TYPES OF ASSESSMENTS	
	[WITHDRAWN: Incorporated into CA-02.]	

CA-07(03)	CONTINUOUS MONITORING | TREND ANALYSES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-07(03)[01]	trend analysis is employed to determine if control implementations used in the continuous monitoring process need to be modified based on empirical data;
	CA-07(03)[02]	trend analysis is employed to determine if the frequency of continuous monitoring activities used in the continuous monitoring process needs to be modified based on empirical data;
	CA-07(03)[03]	trend analysis is employed to determine if the types of activities used in the continuous monitoring process need to be modified based on empirical data.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-07(03)-Examine	[SELECT FROM: Organizational continuous monitoring strategy; system-level continuous monitoring strategy; assessment, authorization, and monitoring policy; procedures addressing continuous monitoring of system controls; privacy controls; assessment report; plan of action and milestones; system monitoring records; impact analyses; status reports; system security plan; privacy plan; other relevant documents or records].
	CA-07(03)-Interview	[SELECT FROM: Organizational personnel with continuous monitoring responsibilities; organizational personnel with information security and privacy responsibilities].
	CA-07(03)-Test	[SELECT FROM: Mechanisms supporting trend analyses].

CA-07(04)	CONTINUOUS MONITORING | RISK MONITORING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-07(04)	risk monitoring is an integral part of the continuous monitoring strategy;
	CA-07(04)(a)	effectiveness monitoring is included in risk monitoring;
	CA-07(04)(b)	compliance monitoring is included in risk monitoring;
	CA-07(04)(c)	change monitoring is included in risk monitoring.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-07(04)-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; organizational continuous monitoring strategy; system-level continuous monitoring strategy; procedures addressing continuous monitoring of system controls; assessment report; plan of action and milestones; system monitoring records; impact analyses; status reports; system security plan; privacy plan; other relevant documents or records].
	CA-07(04)-Interview	[SELECT FROM: Organizational personnel with continuous monitoring responsibilities; organizational personnel with information security and privacy responsibilities].
	CA-07(04)-Test	[SELECT FROM: Mechanisms supporting risk monitoring].

CA-07(05)	CONTINUOUS MONITORING | CONSISTENCY ANALYSIS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-07(05)_ODP[01]	***actions to validate that policies are established are defined;***
	CA-07(05)_ODP[02]	***actions to validate that implemented controls are operating in a consistent manner are defined;***
	CA-07(05)[01]	***<CA-07(05)_ODP[01] actions>*** are employed to validate that policies are established;
	CA-07(05)[02]	***<CA-07(05)_ODP[02] actions>*** are employed to validate that implemented controls are operating in a consistent manner.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-07(05)-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; organizational continuous monitoring strategy; system-level continuous monitoring strategy; procedures addressing continuous monitoring of system security controls; assessment report; plan of action and milestones; system monitoring records; security impact analyses; status reports; system security plan; other relevant documents or records].
	CA-07(05)-Interview	[SELECT FROM: Organizational personnel with continuous monitoring responsibilities; organizational personnel with information security and privacy responsibilities].
	CA-07(05)-Test	[SELECT FROM: Mechanisms supporting consistency analyses].

CA-07(06)	CONTINUOUS MONITORING | AUTOMATION SUPPORT FOR MONITORING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-07(06)_ODP	***automated mechanisms used to ensure the accuracy, currency, and availability of monitoring results for the system are defined;***
	CA-07(06)	***<CA-07(06)_ODP automated mechanisms>*** are used to ensure the accuracy, currency, and availability of monitoring results for the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-07(06)-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; organizational continuous monitoring strategy; system-level continuous monitoring strategy; procedures addressing continuous monitoring of system controls; assessment report; plan of action and milestones; system monitoring records; impact analyses; status reports; system security plan; privacy plan; other relevant documents or records].
	CA-07(06)-Interview	[SELECT FROM: Organizational personnel with continuous monitoring responsibilities; organizational personnel with information security and privacy responsibilities].
	CA-07(06)-Test	[SELECT FROM: Mechanisms supporting automated monitoring].

CA-08	PENETRATION TESTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-08_ODP[01]	***frequency at which to conduct penetration testing on systems or system components is defined;***
	CA-08_ODP[02]	***systems or system components on which penetration testing is to be conducted are defined;***
	CA-08	penetration testing is conducted ***<CA-08_ODP[01] frequency>*** on ***<CA-08_ODP[02] system(s) or system components>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-08-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; procedures addressing penetration testing; assessment plan; penetration test report; assessment report; assessment evidence; system security plan; privacy plan; other relevant documents or records].
	CA-08-Interview	[SELECT FROM: Organizational personnel with control assessment responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	CA-08-Test	[SELECT FROM: Mechanisms supporting penetration testing].

CA-08(01)	PENETRATION TESTING | INDEPENDENT PENETRATION TESTING AGENT OR TEAM	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-08(01)	an independent penetration testing agent or team is employed to perform penetration testing on the system or system components.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-08(01)-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; procedures addressing penetration testing; assessment plan; penetration test report; assessment report; security assessment evidence; system security plan; privacy plan; other relevant documents or records].
	CA-08(01)-Interview	[SELECT FROM: Organizational personnel with assessment responsibilities; organizational personnel with information security and privacy responsibilities].

CA-08(02)	PENETRATION TESTING | RED TEAM EXERCISES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-08(02)_ODP	***red team exercises to simulate attempts by adversaries to compromise organizational systems are defined;***
	CA-08(02)	***<CA-08(02)_ODP red team exercises>*** are employed to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement.

CA-08(02)	PENETRATION TESTING | RED TEAM EXERCISES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-08(02)-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; procedures addressing penetration testing; procedures addressing red team exercises; assessment plan; results of red team exercises; penetration test report; assessment report; rules of engagement; assessment evidence; system security plan; privacy plan; other relevant documents or records].
	CA-08(02)-Interview	[SELECT FROM: Organizational personnel with assessment responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	CA-08(02)-Test	[SELECT FROM: Mechanisms supporting the employment of red team exercises].

CA-08(03)	PENETRATION TESTING | FACILITY PENETRATION TESTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-08(03)_ODP[01]	***frequency at which to employ penetration testing that attempts to bypass or circumvent controls associated with physical access points to the facility is defined;***
	CA-08(03)_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {announced; unannounced};***
	CA-08(03)	the penetration testing process includes ***<CA-08(03)_ODP[01] frequency> <CA-08(03)_ODP[02] SELECTED PARAMETER VALUE(S)>*** attempts to bypass or circumvent controls associated with physical access points to facility.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-08(03)-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; procedures addressing penetration testing; procedures addressing red team exercises; assessment plan; results of red team exercises; penetration test report; assessment report; rules of engagement; assessment evidence; system security plan; privacy plan; other relevant documents or records].
	CA-08(03)-Interview	[SELECT FROM: Organizational personnel with assessment responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	CA-08(03)-Test	[SELECT FROM: Automated mechanisms supporting the employment of red team exercises].

CA-09	INTERNAL SYSTEM CONNECTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-09_ODP[01]	***system components or classes of components requiring internal connections to the system are defined;***
	CA-09_ODP[02]	***conditions requiring termination of internal connections are defined;***

CA-09	INTERNAL SYSTEM CONNECTIONS	
	CA-09_ODP[03]	***frequency at which to review the continued need for each internal connection is defined;***
	CA-09a.	internal connections of ***<CA-09_ODP[01] system components>*** to the system are authorized;
	CA-09b.[01]	for each internal connection, the interface characteristics are documented;
	CA-09b.[02]	for each internal connection, the security requirements are documented;
	CA-09b.[03]	for each internal connection, the privacy requirements are documented;
	CA-09b.[04]	for each internal connection, the nature of the information communicated is documented;
	CA-09c.	internal system connections are terminated after ***<CA-09_ODP[02] conditions>***;
	CA-09d.	the continued need for each internal connection is reviewed ***<CA-09_ODP[03] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-09-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; access control policy; procedures addressing system connections; system and communications protection policy; system design documentation; system configuration settings and associated documentation; list of components or classes of components authorized as internal system connections; assessment report; system audit records; system security plan; privacy plan; other relevant documents or records].
	CA-09-Interview	[SELECT FROM: Organizational personnel with responsibilities for developing, implementing, or authorizing internal system connections; organizational personnel with information security and privacy responsibilities].
	CA-09-Test	[SELECT FROM: Mechanisms supporting internal system connections].

CA-09(01)	INTERNAL SYSTEM CONNECTIONS | COMPLIANCE CHECKS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CA-09(01)[01]	security compliance checks are performed on constituent system components prior to the establishment of the internal connection;
	CA-09(01)[02]	privacy compliance checks are performed on constituent system components prior to the establishment of the internal connection.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CA-09(01)-Examine	[SELECT FROM: Assessment, authorization, and monitoring policy; access control policy; procedures addressing system connections; system and communications protection policy; system design documentation; system configuration settings and associated documentation; list of components or classes of components authorized as internal system connections; assessment report; system audit records; system security plan; privacy plan; other relevant documents or records].
	CA-09(01)-Interview	[SELECT FROM: Organizational personnel with responsibilities for developing, implementing, or authorizing internal system connections; organizational personnel with information security and privacy responsibilities].

CA-09(01)	INTERNAL SYSTEM CONNECTIONS | COMPLIANCE CHECKS	
	CA-09(01)-Test	[SELECT FROM: Mechanisms supporting compliance checks].

4.5 CONFIGURATION MANAGEMENT

CM-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-01_ODP[01]	***personnel or roles to whom the configuration management policy is to be disseminated is/are defined;***
	CM-01_ODP[02]	***personnel or roles to whom the configuration management procedures are to be disseminated is/are defined;***
	CM-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	CM-01_ODP[04]	***an official to manage the configuration management policy and procedures is defined;***
	CM-01_ODP[05]	***the frequency at which the current configuration management policy is reviewed and updated is defined;***
	CM-01_ODP[06]	***events that would require the current configuration management policy to be reviewed and updated are defined;***
	CM-01_ODP[07]	***the frequency at which the current configuration management procedures are reviewed and updated is defined;***
	CM-01_ODP[08]	***events that would require configuration management procedures to be reviewed and updated are defined;***
	CM-01a.[01]	a configuration management policy is developed and documented;
	CM-01a.[02]	the configuration management policy is disseminated to ***<CM-01_ODP[01] personnel or roles>***;
	CM-01a.[03]	configuration management procedures to facilitate the implementation of the configuration management policy and associated configuration management controls are developed and documented;
	CM-01a.[04]	the configuration management procedures are disseminated to ***<CM-01_ODP[02] personnel or roles>***;
	CM-01a.01(a)[01]	the ***<CM-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** of the configuration management policy addresses purpose;
	CM-01a.01(a)[02]	the ***<CM-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** of the configuration management policy addresses scope;
	CM-01a.01(a)[03]	the ***<CM-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** of the configuration management policy addresses roles;
	CM-01a.01(a)[04]	the ***<CM-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** of the configuration management policy addresses responsibilities;
	CM-01a.01(a)[05]	the ***<CM-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** of the configuration management policy addresses management commitment;
	CM-01a.01(a)[06]	the ***<CM-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** of the configuration management policy addresses coordination among organizational entities;

CM-01	POLICY AND PROCEDURES	
	CM-01a.01(a)[07]	the ***<CM-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** of the configuration management policy addresses compliance;
	CM-01a.01(b)	the configuration management policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines;
	CM-01b.	the ***<CM-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the configuration management policy and procedures;
	CM-01c.01[01]	the current configuration management policy is reviewed and updated ***<CM-01_ODP[05] frequency>***;
	CM-01c.01[02]	the current configuration management policy is reviewed and updated following ***<CM-01_ODP[06] events>***;
	CM-01c.02[01]	the current configuration management procedures are reviewed and updated ***<CM-01_ODP[07] frequency>***;
	CM-01c.02[02]	the current configuration management procedures are reviewed and updated following ***<CM-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-01-Examine	[SELECT FROM: Configuration management policy and procedures; security and privacy program policies and procedures; assessment or audit findings; documentation of security incidents or breaches; system security plan; privacy plan; risk management strategy; other relevant artifacts, documents, or records].
	CM-01-Interview	[SELECT FROM: Organizational personnel with configuration management responsibilities; organizational personnel with information security and privacy responsibilities].

CM-02	BASELINE CONFIGURATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-02_ODP[01]	***the frequency of baseline configuration review and update is defined;***
	CM-02_ODP[02]	***the circumstances requiring baseline configuration review and update are defined;***
	CM-02a.[01]	a current baseline configuration of the system is developed and documented;
	CM-02a.[02]	a current baseline configuration of the system is maintained under configuration control;
	CM-02b.01	the baseline configuration of the system is reviewed and updated ***<CM-02_ODP[01] frequency>***;
	CM-02b.02	the baseline configuration of the system is reviewed and updated when required due to ***<CM-02_ODP[02] circumstances>***;
	CM-02b.03	the baseline configuration of the system is reviewed and updated when system components are installed or upgraded.

CM-02	BASELINE CONFIGURATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-02-Examine	[SELECT FROM: Configuration management policy; procedures addressing the baseline configuration of the system; configuration management plan; enterprise architecture documentation; system design documentation; system security plan; privacy plan; system architecture and configuration documentation; system configuration settings and associated documentation; system component inventory; change control records; other relevant documents or records].
	CM-02-Interview	[SELECT FROM: Organizational personnel with configuration management responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	CM-02-Test	[SELECT FROM: Organizational processes for managing baseline configurations; mechanisms supporting configuration control of the baseline configuration].

CM-02(01)	BASELINE CONFIGURATION | REVIEWS AND UPDATES
	[WITHDRAWN: Incorporated into CM-02.]

CM-02(02)	BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-02(02)_ODP	***automated mechanisms for maintaining baseline configuration of the system are defined;***
	CM-02(02)[01]	the currency of the baseline configuration of the system is maintained using ***<CM-02(02)_ODP automated mechanisms>***;
	CM-02(02)[02]	the completeness of the baseline configuration of the system is maintained using ***<CM-02(02)_ODP automated mechanisms>***;
	CM-02(02)[03]	the accuracy of the baseline configuration of the system is maintained using ***<CM-02(02)_ODP automated mechanisms>***;
	CM-02(02)[04]	the availability of the baseline configuration of the system is maintained using ***<CM-02(02)_ODP automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-02(02)-Examine	[SELECT FROM: Configuration management policy; procedures addressing the baseline configuration of the system; configuration management plan; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; system component inventory; configuration change control records; system security plan; other relevant documents or records].
	CM-02(02)-Interview	[SELECT FROM: Organizational personnel with configuration management responsibilities; organizational personnel with information security responsibilities; system/network administrators].

CM-02(02)	BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY	
	CM-02(02)-Test	[SELECT FROM: Organizational processes for managing baseline configurations; automated mechanisms implementing baseline configuration maintenance].

CM-02(03)	BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-02(03)_ODP	***the number of previous baseline configuration versions to be retained is defined;***
	CM-02(03)	***<CM-02(03)_ODP number>*** of previous baseline configuration version(s) of the system is/are retained to support rollback.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-02(03)-Examine	[SELECT FROM: Configuration management policy; procedures addressing the baseline configuration of the system; configuration management plan; system architecture and configuration documentation; system configuration settings and associated documentation; copies of previous baseline configuration versions; system security plan; other relevant documents or records].
	CM-02(03)-Interview	[SELECT FROM: Organizational personnel with configuration management responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	CM-02(03)-Test	[SELECT FROM: Organizational processes for managing baseline configurations].

CM-02(04)	BASELINE CONFIGURATION | UNAUTHORIZED SOFTWARE
	[WITHDRAWN: Incorporated into CM-07(04).]

CM-02(05)	BASELINE CONFIGURATION | AUTHORIZED SOFTWARE
	[WITHDRAWN: Incorporated into CM-07(05).]

CM-02(06)	BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-02(06)[01]	a baseline configuration for system development environments that is managed separately from the operational baseline configuration is maintained;
	CM-02(06)[02]	a baseline configuration for test environments that is managed separately from the operational baseline configuration is maintained.

CM-02(06)	BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-02(06)-Examine	[SELECT FROM: Configuration management policy; procedures addressing the baseline configuration of the system; configuration management plan; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; system security plan; other relevant documents or records].
	CM-02(06)-Interview	[SELECT FROM: Organizational personnel with configuration management responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	CM-02(06)-Test	[SELECT FROM: Organizational processes for managing baseline configurations; mechanisms implementing separate baseline configurations for development, test, and operational environments].

CM-02(07)	BASELINE CONFIGURATION | CONFIGURE SYSTEMS AND COMPONENTS FOR HIGH-RISK AREAS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-02(07)_ODP[01]	***the systems or system components to be issued when individuals travel to high-risk areas are defined;***
	CM-02(07)_ODP[02]	***configurations for systems or system components to be issued when individuals travel to high-risk areas are defined;***
	CM-02(07)_ODP[03]	***the controls to be applied when the individuals return from travel are defined;***
	CM-02(07)(a)	***<CM-02(07)_ODP[01] systems or system components>*** with ***<CM-02(07)_ODP[02] configurations>*** are issued to individuals traveling to locations that the organization deems to be of significant risk;
	CM-02(07)(b)	***<CM-02(07)_ODP[03] controls>*** are applied to the systems or system components when the individuals return from travel.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-02(07)-Examine	[SELECT FROM: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the system; procedures addressing system component installations and upgrades; system architecture and configuration documentation; system configuration settings and associated documentation; system component inventory; records of system baseline configuration reviews and updates; system component installations/upgrades and associated records; change control records; system security plan; other relevant documents or records].
	CM-02(07)-Interview	[SELECT FROM: Organizational personnel with configuration management responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	CM-02(07)-Test	[SELECT FROM: Organizational processes for managing baseline configurations].

CM-03	CONFIGURATION CHANGE CONTROL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-03_ODP[01]	***the time period to retain records of configuration-controlled changes is defined;***
	CM-03_ODP[02]	***the configuration change control element responsible for coordinating and overseeing change control activities is defined;***
	CM-03_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {<CM-03_ODP[04] frequency>; when <CM-03_ODP[05] configuration change conditions>};***
	CM-03_ODP[04]	***the frequency at which the configuration control element convenes is defined (if selected);***
	CM-03_ODP[05]	***configuration change conditions that prompt the configuration control element to convene are defined (if selected);***
	CM-03a.	the types of changes to the system that are configuration-controlled are determined and documented;
	CM-03b.[01]	proposed configuration-controlled changes to the system are reviewed;
	CM-03b.[02]	proposed configuration-controlled changes to the system are approved or disapproved with explicit consideration for security and privacy impact analyses;
	CM-03c.	configuration change decisions associated with the system are documented;
	CM-03d.	approved configuration-controlled changes to the system are implemented;
	CM-03e.	records of configuration-controlled changes to the system are retained for ***<CM-03_ODP[01] time period>***;
	CM-03f.[01]	activities associated with configuration-controlled changes to the system are monitored;
	CM-03f.[02]	activities associated with configuration-controlled changes to the system are reviewed;
	CM-03g.[01]	configuration change control activities are coordinated and overseen by ***<CM-03_ODP[02] configuration change control element>***;
	CM-03g.[02]	the configuration control element convenes ***<CM-03_ODP[03] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-03-Examine	[SELECT FROM: Configuration management policy; procedures addressing system configuration change control; configuration management plan; system architecture and configuration documentation; change control records; system audit records; change control audit and review reports; agenda/minutes/documentation from configuration change control oversight meetings; system security plan; privacy plan; privacy impact assessments; system of records notices; other relevant documents or records].
	CM-03-Interview	[SELECT FROM: Organizational personnel with configuration change control responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; members of change control board or similar].

CM-03	CONFIGURATION CHANGE CONTROL	
	CM-03-Test	[SELECT FROM: Organizational processes for configuration change control; mechanisms that implement configuration change control].

CM-03(01)	CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENTATION, NOTIFICATION, AND PROHIBITION OF CHANGES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-03(01)_ODP[01]	***mechanisms used to automate configuration change control are defined;***
	CM-03(01)_ODP[02]	***approval authorities to be notified of and request approval for proposed changes to the system are defined;***
	CM-03(01)_ODP[03]	***the time period after which to highlight changes that have not been approved or disapproved is defined;***
	CM-03(01)_ODP[04]	***personnel to be notified when approved changes are complete is/are defined;***
	CM-03(01)(a)	***<CM-03(01)_ODP[01] automated mechanisms>*** are used to document proposed changes to the system;
	CM-03(01)(b)	***<CM-03(01)_ODP[01] automated mechanisms>*** are used to notify ***<CM-03(01)_ODP[02] approval authorities>*** of proposed changes to the system and request change approval;
	CM-03(01)(c)	***<CM-03(01)_ODP[01] automated mechanisms>*** are used to highlight proposed changes to the system that have not been approved or disapproved within ***<CM-03(01)_ODP[03] time period>***;
	CM-03(01)(d)	***<CM-03(01)_ODP[01] automated mechanisms>*** are used to prohibit changes to the system until designated approvals are received;
	CM-03(01)(e)	***<CM-03(01)_ODP[01] automated mechanisms>*** are used to document all changes to the system;
	CM-03(01)(f)	***<CM-03(01)_ODP[01] automated mechanisms>*** are used to notify ***<CM-03(01)_ODP[04] personnel>*** when approved changes to the system are completed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-03(01)-Examine	[SELECT FROM: Configuration management policy; procedures addressing system configuration change control; configuration management plan; system design documentation; system architecture and configuration documentation; automated configuration control mechanisms; system configuration settings and associated documentation; change control records; system audit records; change approval requests; change approvals; system security plan; other relevant documents or records].
	CM-03(01)-Interview	[SELECT FROM: Organizational personnel with configuration change control responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; members of change control board or similar].
	CM-03(01)-Test	[SELECT FROM: Organizational processes for configuration change control; automated mechanisms implementing configuration change control activities].

CM-03(02)	CONFIGURATION CHANGE CONTROL | TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-03(02)[01]	changes to the system are tested before finalizing the implementation of the changes;
	CM-03(02)[02]	changes to the system are validated before finalizing the implementation of the changes;
	CM-03(02)[03]	changes to the system are documented before finalizing the implementation of the changes.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-03(02)-Examine	[SELECT FROM: Configuration management policy; configuration management plan; procedures addressing system configuration change control; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; test records; validation records; change control records; system audit records; system security plan; other relevant documents or records].
	CM-03(02)-Interview	[SELECT FROM: Organizational personnel with configuration change control responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; members of change control board or similar].
	CM-03(02)-Test	[SELECT FROM: Organizational processes for configuration change control; mechanisms supporting and/or implementing, testing, validating, and documenting system changes].

CM-03(03)	CONFIGURATION CHANGE CONTROL | AUTOMATED CHANGE IMPLEMENTATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-03(03)_ODP	***mechanisms used to automate the implementation of changes and deployment of the updated baseline across the installed base are defined;***
	CM-03(03)[01]	changes to the current system baseline are implemented using ***<CM-03(03)_ODP automated mechanisms>***;
	CM-03(03)[02]	the updated baseline is deployed across the installed base using ***<CM-03(03)_ODP automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-03(03)-Examine	[SELECT FROM: Configuration management policy; configuration management plan; procedures addressing system configuration change control; system design documentation; system architecture and configuration documentation; automated configuration control mechanisms; change control records; system component inventory; system audit records; system security plan; other relevant documents or records].

CM-03(03)	CONFIGURATION CHANGE CONTROL | AUTOMATED CHANGE IMPLEMENTATION	
	CM-03(03)-Interview	[SELECT FROM: Organizational personnel with configuration change control responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; members of change control board or similar].
	CM-03(03)-Test	[SELECT FROM: Organizational processes for configuration change control; automated mechanisms implementing changes to current system baseline].

CM-03(04)	CONFIGURATION CHANGE CONTROL | SECURITY AND PRIVACY REPRESENTATIVES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-03(04)_ODP[01]	***security representatives required to be members of the change control element are defined;***
	CM-03(04)_ODP[02]	***privacy representatives required to be members of the change control element are defined;***
	CM-03(04)_ODP[03]	***the configuration change control element of which the security and privacy representatives are to be members is defined;***
	CM-03(04)[01]	***<CM-03(04)_ODP[01] security representatives>*** are required to be members of the ***<CM-03(04)_ODP[03] configuration change control element>***;
	CM-03(04)[02]	***<CM-03(04)_ODP[02] privacy representatives>*** are required to be members of the ***<CM-03(04)_ODP[03] configuration change control element>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-03(04)-Examine	[SELECT FROM: Configuration management policy; procedures addressing system configuration change control; configuration management plan; system security plan; privacy plan; other relevant documents or records].
	CM-03(04)-Interview	[SELECT FROM: Organizational personnel with configuration change control responsibilities; organizational personnel with information security and privacy responsibilities; members of change control board or similar].
	CM-03(04)-Test	[SELECT FROM: Organizational processes for configuration change control].

CM-03(05)	CONFIGURATION CHANGE CONTROL | AUTOMATED SECURITY RESPONSE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-03(05)_ODP	***security responses to be automatically implemented are defined;***
	CM-03(05)	***<CM-03(05)_ODP security responses>*** are automatically implemented if baseline configurations are changed in an unauthorized manner.

CM-03(05)	CONFIGURATION CHANGE CONTROL | AUTOMATED SECURITY RESPONSE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-03(05)-Examine	[SELECT FROM: System security plan; configuration management policy; procedures addressing system configuration change control; configuration management plan; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; alerts/notifications of unauthorized baseline configuration changes; system audit records; other relevant documents or records].
	CM-03(05)-Interview	[SELECT FROM: Organizational personnel with configuration change control responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; members of change control board or similar].
	CM-03(05)-Test	[SELECT FROM: Organizational processes for configuration change control; automated mechanisms implementing security responses to unauthorized changes to the baseline configurations].

CM-03(06)	CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-03(06)_ODP	***controls provided by cryptographic mechanisms that are to be under configuration management are defined;***
	CM-03(06)	cryptographic mechanisms used to provide ***<CM-03(06)_ODP controls>*** are under configuration management.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-03(06)-Examine	[SELECT FROM: Configuration management policy; procedures addressing system configuration change control; configuration management plan; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; system security plan; other relevant documents or records].
	CM-03(06)-Interview	[SELECT FROM: Organizational personnel with configuration change control responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; members of change control board or similar].
	CM-03(06)-Test	[SELECT FROM: Organizational processes for configuration change control; cryptographic mechanisms implementing organizational security safeguards (controls)].

CM-03(07)	CONFIGURATION CHANGE CONTROL | REVIEW SYSTEM CHANGES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-03(07)_ODP[01]	***the frequency at which changes are to be reviewed is defined;***
	CM-03(07)_ODP[02]	***the circumstances under which changes are to be reviewed are defined;***

CM-03(07)	CONFIGURATION CHANGE CONTROL | REVIEW SYSTEM CHANGES	
	CM-03(07)	changes to the system are reviewed ***<CM-03(07)_ODP[01] frequency>*** or when ***<CM-03(07)_ODP[02] circumstances>*** to determine whether unauthorized changes have occurred.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-03(07)-Examine	[SELECT FROM: Configuration management policy; procedures addressing system configuration change control; configuration management plan; change control records; system architecture and configuration documentation; system configuration settings and associated documentation; system audit records; system component inventory; system security plan; other relevant documents or records].
	CM-03(07)-Interview	[SELECT FROM: Organizational personnel with configuration change control responsibilities; organizational personnel with security responsibilities; system/network administrators; members of change control board or similar].
	CM-03(07)-Test	[SELECT FROM: Organizational processes for configuration change control; mechanisms implementing audit records for changes].

CM-03(08)	CONFIGURATION CHANGE CONTROL | PREVENT OR RESTRICT CONFIGURATION CHANGES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-03(08)_ODP	***the circumstances under which changes are to be prevented or restricted are defined;***
	CM-03(08)	changes to the configuration of the system are prevented or restricted under ***<CM-03(08)_ODP circumstances>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-03(08)-Examine	[SELECT FROM: Configuration management policy; procedures addressing system configuration change control; configuration management plan; change control records; system architecture and configuration documentation; system configuration settings and associated documentation; system component inventory; system audit records; system security plan; other relevant documents or records].

CM-04	IMPACT ANALYSES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-04[01]	changes to the system are analyzed to determine potential security impacts prior to change implementation;
	CM-04[02]	changes to the system are analyzed to determine potential privacy impacts prior to change implementation.

CM-04	IMPACT ANALYSES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-04-Examine	[SELECT FROM: Configuration management policy; procedures addressing security impact analyses for changes to the system; procedures addressing privacy impact analyses for changes to the system; configuration management plan; security impact analysis documentation; privacy impact analysis documentation; privacy impact assessment; privacy risk assessment documentation, system design documentation; analysis tools and associated outputs; change control records; system audit records; system security plan; privacy plan; other relevant documents or records].
	CM-04-Interview	[SELECT FROM: Organizational personnel with responsibility for conducting security impact analyses; organizational personnel with responsibility for conducting privacy impact analyses; organizational personnel with information security and privacy responsibilities; system developer; system/network administrators; members of change control board or similar].
	CM-04-Test	[SELECT FROM: Organizational processes for security impact analyses; organizational processes for privacy impact analyses].

CM-04(01)	IMPACT ANALYSES | SEPARATE TEST ENVIRONMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-04(01)[01]	changes to the system are analyzed in a separate test environment before implementation in an operational environment;
	CM-04(01)[02]	changes to the system are analyzed for security impacts due to flaws;
	CM-04(01)[03]	changes to the system are analyzed for privacy impacts due to flaws;
	CM-04(01)[04]	changes to the system are analyzed for security impacts due to weaknesses;
	CM-04(01)[05]	changes to the system are analyzed for privacy impacts due to weaknesses;
	CM-04(01)[06]	changes to the system are analyzed for security impacts due to incompatibility;
	CM-04(01)[07]	changes to the system are analyzed for privacy impacts due to incompatibility;
	CM-04(01)[08]	changes to the system are analyzed for security impacts due to intentional malice;
	CM-04(01)[09]	changes to the system are analyzed for privacy impacts due to intentional malice.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-04(01)-Examine	[SELECT FROM: Configuration management policy; procedures addressing security impact analyses for changes to the system; procedures addressing privacy impact analyses for changes to the system; configuration management plan; security impact analysis documentation; privacy impact analysis documentation; privacy impact assessment; privacy risk assessment documentation; analysis tools and associated outputs system design documentation; system architecture and configuration documentation; change control records; procedures addressing the authority to test with PII; system audit records; documentation of separate test and operational environments; system security plan; privacy plan; other relevant documents or records].

CM-04(01)	IMPACT ANALYSES | SEPARATE TEST ENVIRONMENTS	
	CM-04(01)-Interview	[SELECT FROM: Organizational personnel with responsibility for conducting security and privacy impact analyses; organizational personnel with information security and privacy responsibilities; system/network administrators; members of change control board or similar].
	CM-04(01)-Test	[SELECT FROM: Organizational processes for security and privacy impact analyses; mechanisms supporting and/or implementing security and privacy impact analyses of changes].

CM-04(02)	IMPACT ANALYSES | VERIFICATION OF CONTROLS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-04(02)[01]	the impacted controls are implemented correctly with regard to meeting the security requirements for the system after system changes;
	CM-04(02)[02]	the impacted controls are implemented correctly with regard to meeting the privacy requirements for the system after system changes;
	CM-04(02)[03]	the impacted controls are operating as intended with regard to meeting the security requirements for the system after system changes;
	CM-04(02)[04]	the impacted controls are operating as intended with regard to meeting the privacy requirements for the system after system changes;
	CM-04(02)[05]	the impacted controls are producing the desired outcome with regard to meeting the security requirements for the system after system changes;
	CM-04(02)[06]	the impacted controls are producing the desired outcome with regard to meeting the privacy requirements for the system after system changes.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-04(02)-Examine	[SELECT FROM: Configuration management policy; procedures addressing security impact analyses for changes to the system; procedures addressing privacy impact analyses for changes to the system; privacy risk assessment documentation; configuration management plan; security and privacy impact analysis documentation; privacy impact assessment; analysis tools and associated outputs; change control records; control assessment results; system audit records; system component inventory; system security plan; privacy plan; other relevant documents or records].
	CM-04(02)-Interview	[SELECT FROM: Organizational personnel with responsibility for conducting security and privacy impact analyses; organizational personnel with information security and privacy responsibilities; system/network administrators; security and privacy assessors].
	CM-04(02)-Test	[SELECT FROM: Organizational processes for security and privacy impact analyses; mechanisms supporting and/or implementing security and privacy impact analyses of changes].

CM-05	ACCESS RESTRICTIONS FOR CHANGE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-05[01]	physical access restrictions associated with changes to the system are defined and documented;
	CM-05[02]	physical access restrictions associated with changes to the system are approved;
	CM-05[03]	physical access restrictions associated with changes to the system are enforced;
	CM-05[04]	logical access restrictions associated with changes to the system are defined and documented;
	CM-05[05]	logical access restrictions associated with changes to the system are approved;
	CM-05[06]	logical access restrictions associated with changes to the system are enforced.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-05-Examine	[SELECT FROM: Configuration management policy; procedures addressing access restrictions for changes to the system; configuration management plan; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; logical access approvals; physical access approvals; access credentials; change control records; system audit records; system security plan; other relevant documents or records].
	CM-05-Interview	[SELECT FROM: Organizational personnel with logical access control responsibilities; organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	CM-05-Test	[SELECT FROM: Organizational processes for managing access restrictions to change; mechanisms supporting, implementing, or enforcing access restrictions associated with changes to the system].

CM-05(01)	ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT AND AUDIT RECORDS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-05(01)_ODP	***mechanisms used to automate the enforcement of access restrictions are defined;***
	CM-05(01)(a)	access restrictions for change are enforced using ***<CM-05(01)_ODP automated mechanisms>***;
	CM-05(01)(b)	audit records of enforcement actions are automatically generated.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-05(01)-Examine	[SELECT FROM: Configuration management policy; procedures addressing access restrictions for changes to the system; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; change control records; system audit records; system security plan; other relevant documents or records].

CM-05(01)	ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT AND AUDIT RECORDS	
	CM-05(01)-Interview	[SELECT FROM: Organizational personnel with logical access control responsibilities; organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	CM-05(01)-Test	[SELECT FROM: Organizational processes for managing access restrictions to change; automated mechanisms implementing the enforcement of access restrictions for changes to the system; automated mechanisms supporting auditing of enforcement actions].

CM-05(02)	ACCESS RESTRICTIONS FOR CHANGE | REVIEW SYSTEM CHANGES
	[WITHDRAWN: Incorporated into CM-03(07).]

CM-05(03)	ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS
	[WITHDRAWN: Moved to CM-14.]

CM-05(04)	ACCESS RESTRICTIONS FOR CHANGE | DUAL AUTHORIZATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-05(04)_ODP[01]	***system components requiring dual authorization for changes are defined;***
	CM-05(04)_ODP[02]	***system-level information requiring dual authorization for changes is defined;***
	CM-05(04)[01]	dual authorization for implementing changes to ***<CM-05(04)_ODP[01] system components>*** is enforced;
	CM-05(04)[02]	dual authorization for implementing changes to ***<CM-05(04)_ODP[02] system-level information>*** is enforced.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-05(04)-Examine	[SELECT FROM: Configuration management policy; procedures addressing access restrictions for changes to the system; configuration management plan; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; change control records; system audit records; system component inventory; system information types information; system security plan; other relevant documents or records].
	CM-05(04)-Interview	[SELECT FROM: Organizational personnel with dual authorization enforcement responsibilities for implementing system changes; organizational personnel with information security responsibilities; system/network administrators].
	CM-05(04)-Test	[SELECT FROM: Organizational processes for managing access restrictions to change; mechanisms implementing dual authorization enforcement].

CM-05(05)	ACCESS RESTRICTIONS FOR CHANGE | PRIVILEGE LIMITATION FOR PRODUCTION AND OPERATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-05(05)_ODP[01]	***frequency at which to review privileges is defined;***
	CM-05(05)_ODP[02]	***frequency at which to reevaluate privileges is defined;***
	CM-05(05)(a)[01]	privileges to change system components within a production or operational environment are limited;
	CM-05(05)(a)[02]	privileges to change system-related information within a production or operational environment are limited;
	CM-05(05)(b)[01]	privileges are reviewed ***<CM-05(05)_ODP[01] frequency>***;
	CM-05(05)(b)[02]	privileges are reevaluated ***<CM-05(05)_ODP[02] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-05(05)-Examine	[SELECT FROM: Configuration management policy; procedures addressing access restrictions for changes to the system; configuration management plan; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; user privilege reviews; user privilege recertifications; system component inventory; change control records; system audit records; system security plan; other relevant documents or records].
	CM-05(05)-Interview	[SELECT FROM: Organizational personnel with information security responsibilities; system/network administrators].
	CM-05(05)-Test	[SELECT FROM: Organizational processes for managing access restrictions to change; mechanisms supporting and/or implementing access restrictions for change].

CM-05(06)	ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-05(06)	privileges to change software resident within software libraries are limited.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-05(06)-Examine	[SELECT FROM: Configuration management policy; procedures addressing access restrictions for changes to the system; configuration management plan; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; system component inventory; change control records; system audit records; system security plan; other relevant documents or records].
	CM-05(06)-Interview	[SELECT FROM: Organizational personnel with information security responsibilities; system/network administrators].
	CM-05(06)-Test	[SELECT FROM: Organizational processes for managing access restrictions to change; mechanisms supporting and/or implementing access restrictions for change].

CM-05(07)	ACCESS RESTRICTIONS FOR CHANGE | AUTOMATIC IMPLEMENTATION OF SECURITY SAFEGUARDS
	[WITHDRAWN: Incorporated into SI-07.]

CM-06	CONFIGURATION SETTINGS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-06_ODP[01]	***common secure configurations to establish and document configuration settings for components employed within the system are defined;***
	CM-06_ODP[02]	***system components for which approval of deviations is needed are defined;***
	CM-06_ODP[03]	***operational requirements necessitating approval of deviations are defined;***
	CM-06a.	configuration settings that reflect the most restrictive mode consistent with operational requirements are established and documented for components employed within the system using ***<CM-06_ODP[01] common secure configurations>***;
	CM-06b.	the configuration settings documented in CM-06a are implemented;
	CM-06c.[01]	any deviations from established configuration settings for ***<CM-06_ODP[02] system components>*** are identified and documented based on ***<CM-06_ODP[03] operational requirements>***;
	CM-06c.[02]	any deviations from established configuration settings for ***<CM-06_ODP[02] system components>*** are approved;
	CM-06d.[01]	changes to the configuration settings are monitored in accordance with organizational policies and procedures;
	CM-06d.[02]	changes to the configuration settings are controlled in accordance with organizational policies and procedures.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-06-Examine	[SELECT FROM: Configuration management policy; procedures addressing configuration settings for the system; configuration management plan; system design documentation; system configuration settings and associated documentation; common secure configuration checklists; system component inventory; evidence supporting approved deviations from established configuration settings; change control records; system data processing and retention permissions; system audit records; system security plan; privacy plan; other relevant documents or records].
	CM-06-Interview	[SELECT FROM: Organizational personnel with security configuration management responsibilities; organizational personnel with privacy configuration management responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	CM-06-Test	[SELECT FROM: Organizational processes for managing configuration settings; mechanisms that implement, monitor, and/or control system configuration settings; mechanisms that identify and/or document deviations from established configuration settings].

CM-06(01)	CONFIGURATION SETTINGS | AUTOMATED MANAGEMENT, APPLICATION, AND VERIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-06(01)_ODP[01]	***system components for which to manage, apply, and verify configuration settings are defined;***
	CM-06(01)_ODP[02]	***automated mechanisms to manage configuration settings are defined;***
	CM-06(01)_ODP[03]	***automated mechanisms to apply configuration settings are defined;***
	CM-06(01)_ODP[04]	***automated mechanisms to verify configuration settings are defined;***
	CM-06(01)[01]	configuration settings for ***<CM-06(01)_ODP[01] system components>*** are managed using ***<CM-06(01)_ODP[02] automated mechanisms>***;
	CM-06(01)[02]	configuration settings for ***<CM-06(01)_ODP[01] system components>*** are applied using ***<CM-06(01)_ODP[03] automated mechanisms>***;
	CM-06(01)[03]	configuration settings for ***<CM-06(01)_ODP[01] system components>*** are verified using ***<CM-06(01)_ODP[04] automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-06(01)-Examine	[SELECT FROM: Configuration management policy; procedures addressing configuration settings for the system; configuration management plan; system design documentation; system configuration settings and associated documentation; system component inventory; common secure configuration checklists; change control records; system audit records; system security plan; privacy plan; other relevant documents or records].
	CM-06(01)-Interview	[SELECT FROM: Organizational personnel with security configuration management responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	CM-06(01)-Test	[SELECT FROM: Organizational processes for managing configuration settings; automated mechanisms implemented to manage, apply, and verify system configuration settings].

CM-06(02)	CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-06(02)_ODP[01]	***actions to be taken upon an unauthorized change are defined;***
	CM-06(02)_ODP[02]	***configuration settings requiring action upon an unauthorized change are defined;***
	CM-06(02)	***<CM-06(02)_ODP[01] actions>*** are taken in response to unauthorized changes to ***<CM-06(02)_ODP[02] configuration settings>***.

CM-06(02)	CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-06(02)-Examine	[SELECT FROM: System security plan; privacy plan; configuration management policy; procedures addressing configuration settings for the system; configuration management plan; system design documentation; system configuration settings and associated documentation; alerts/notifications of unauthorized changes to system configuration settings; system component inventory; documented responses to unauthorized changes to system configuration settings; change control records; system audit records; other relevant documents or records].
	CM-06(02)-Interview	[SELECT FROM: Organizational personnel with security configuration management responsibilities; organizational personnel with security and privacy responsibilities; system/network administrators].
	CM-06(02)-Test	[SELECT FROM: Organizational process for responding to unauthorized changes to system configuration settings; mechanisms supporting and/or implementing actions in response to unauthorized changes].

CM-06(03)	CONFIGURATION SETTINGS | UNAUTHORIZED CHANGE DETECTION
	[WITHDRAWN: Incorporated into SI-07.]

CM-06(04)	CONFIGURATION SETTINGS | CONFORMANCE DEMONSTRATION
	[WITHDRAWN: Incorporated into CM-04.]

CM-07	LEAST FUNCTIONALITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-07_ODP[01]	***mission-essential capabilities for the system are defined;***
	CM-07_ODP[02]	***functions to be prohibited or restricted are defined;***
	CM-07_ODP[03]	***ports to be prohibited or restricted are defined;***
	CM-07_ODP[04]	***protocols to be prohibited or restricted are defined;***
	CM-07_ODP[05]	***software to be prohibited or restricted is defined;***
	CM-07_ODP[06]	***services to be prohibited or restricted are defined;***
	CM-07a.	the system is configured to provide only ***<CM-07_ODP[01] mission-essential capabilities>***;
	CM-07b.[01]	the use of ***<CM-07_ODP[02] functions>*** is prohibited or restricted;
	CM-07b.[02]	the use of ***<CM-07_ODP[03] ports>*** is prohibited or restricted;
	CM-07b.[03]	the use of ***<CM-07_ODP[04] protocols>*** is prohibited or restricted;

CM-07	LEAST FUNCTIONALITY	
	CM-07b.[04]	the use of ***<CM-07_ODP[05] software>*** is prohibited or restricted;
	CM-07b.[05]	the use of ***<CM-07_ODP[06] services>*** is prohibited or restricted.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-07-Examine	[SELECT FROM: Configuration management policy; procedures addressing least functionality in the system; configuration management plan; system design documentation; system configuration settings and associated documentation; system component inventory; common secure configuration checklists; system security plan; other relevant documents or records].
	CM-07-Interview	[SELECT FROM: Organizational personnel with security configuration management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	CM-07-Test	[SELECT FROM: Organizational processes prohibiting or restricting functions, ports, protocols, software, and/or services; mechanisms implementing restrictions or prohibition of functions, ports, protocols, software, and/or services].

CM-07(01)	LEAST FUNCTIONALITY | PERIODIC REVIEW	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-07(01)_ODP[01]	***the frequency at which to review the system to identify unnecessary and/or non-secure functions, ports, protocols, software, and/or services is defined;***
	CM-07(01)_ODP[02]	***functions to be disabled or removed when deemed unnecessary or non-secure are defined;***
	CM-07(01)_ODP[03]	***ports to be disabled or removed when deemed unnecessary or non-secure are defined;***
	CM-07(01)_ODP[04]	***protocols to be disabled or removed when deemed unnecessary or non-secure are defined;***
	CM-07(01)_ODP[05]	***software to be disabled or removed when deemed unnecessary or non-secure is defined;***
	CM-07(01)_ODP[06]	***services to be disabled or removed when deemed unnecessary or non-secure are defined;***
	CM-07(01)(a)	the system is reviewed ***<CM-07(01)_ODP[01] frequency>*** to identify unnecessary and/or non-secure functions, ports, protocols, software, and services:
	CM-07(01)(b)[01]	***<CM-07(01)_ODP[02] functions>*** deemed to be unnecessary and/or non-secure are disabled or removed;
	CM-07(01)(b)[02]	***<CM-07(01)_ODP[03] ports>*** deemed to be unnecessary and/or non-secure are disabled or removed;
	CM-07(01)(b)[03]	***<CM-07(01)_ODP[04] protocols>*** deemed to be unnecessary and/or non-secure are disabled or removed;
	CM-07(01)(b)[04]	***<CM-07(01)_ODP[05] software>*** deemed to be unnecessary and/or non-secure is disabled or removed;

CM-07(01)	LEAST FUNCTIONALITY | PERIODIC REVIEW	
	CM-07(01)(b)[05]	***<CM-07(01)_ODP[06] services>*** deemed to be unnecessary and/or non-secure are disabled or removed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-07(01)-Examine	[SELECT FROM: Configuration management policy; procedures addressing least functionality in the system; configuration management plan; system design documentation; system configuration settings and associated documentation; common secure configuration checklists; documented reviews of functions, ports, protocols, and/or services; change control records; system audit records; system security plan; other relevant documents or records].
	CM-07(01)-Interview	[SELECT FROM: Organizational personnel with responsibilities for reviewing functions, ports, protocols, and services on the system; organizational personnel with information security responsibilities; system/network administrators; system developers].
	CM-07(01)-Test	[SELECT FROM: Organizational processes for reviewing or disabling functions, ports, protocols, and services on the system; mechanisms implementing review and disabling of functions, ports, protocols, and/or services].

CM-07(02)	LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-07(02)_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {<CM-07(02)_ODP[02] policies, rules of behavior, and/or access agreements regarding software program usage and restrictions>; rules authorizing the terms and conditions of software program usage};***
	CM-07(02)_ODP[02]	***policies, rules of behavior, and/or access agreements regarding software program usage and restrictions are defined (if selected);***
	CM-07(02)	program execution is prevented in accordance with ***<CM-07(02)_ODP[01] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-07(02)-Examine	[SELECT FROM: Configuration management policy; procedures addressing least functionality in the system; configuration management plan; system design documentation; system configuration settings and associated documentation; system component inventory; common secure configuration checklists; specifications for preventing software program execution; change control records; system audit records; system security plan; other relevant documents or records].
	CM-07(02)-Interview	[SELECT FROM: Organizational personnel with information security responsibilities; system/network administrators; system developers].
	CM-07(02)-Test	[SELECT FROM: Organizational processes preventing program execution on the system; organizational processes for software program usage and restrictions; mechanisms preventing program execution on the system; mechanisms supporting and/or implementing software program usage and restrictions].

CM-07(03)	LEAST FUNCTIONALITY | REGISTRATION COMPLIANCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-07(03)_ODP	***registration requirements for functions, ports, protocols, and services are defined;***
	CM-07(03)	***<CM-07(03)_ODP registration requirements>*** are complied with.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-07(03)-Examine	[SELECT FROM: System security plan; configuration management policy; procedures addressing least functionality in the system; configuration management plan; system configuration settings and associated documentation; system component inventory; audit and compliance reviews; system audit records; other relevant documents or records].
	CM-07(03)-Interview	[SELECT FROM: Organizational personnel with security responsibilities; system/network administrators; system developers].
	CM-07(03)-Test	[SELECT FROM: Organizational processes ensuring compliance with registration requirements for functions, ports, protocols, and/or services; mechanisms implementing compliance with registration requirements for functions, ports, protocols, and/or services].

CM-07(04)	LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE — DENY-BY-EXCEPTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-07(04)_ODP[01]	***software programs not authorized to execute on the system are defined;***
	CM-07(04)_ODP[02]	***frequency at which to review and update the list of unauthorized software programs is defined;***
	CM-07(04)(a)	***<CM-07(04)_ODP[01] software programs>*** are identified;
	CM-07(04)(b)	an allow-all, deny-by-exception policy is employed to prohibit the execution of unauthorized software programs on the system;
	CM-07(04)(c)	the list of unauthorized software programs is reviewed and updated ***<CM-07(04)_ODP[02] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-07(04)-Examine	[SELECT FROM: Configuration management policy; procedures addressing least functionality in the system; configuration management plan; system design documentation; system configuration settings and associated documentation; list of software programs not authorized to execute on the system; system component inventory; common secure configuration checklists; review and update records associated with list of unauthorized software programs; change control records; system audit records; system security plan; other relevant documents or records].
	CM-07(04)-Interview	[SELECT FROM: Organizational personnel with responsibilities for identifying software not authorized to execute on the system; organizational personnel with information security responsibilities; system/network administrators].

CM-07(04)	LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE — DENY-BY-EXCEPTION	
	CM-07(04)-Test	[SELECT FROM: Organizational process for identifying, reviewing, and updating programs not authorized to execute on the system; organizational process for implementing unauthorized software policy; mechanisms supporting and/or implementing unauthorized software policy].

CM-07(05)	LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE — ALLOW-BY-EXCEPTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-07(05)_ODP[01]	***software programs authorized to execute on the system are defined;***
	CM-07(05)_ODP[02]	***frequency at which to review and update the list of authorized software programs is defined;***
	CM-07(05)(a)	***<CM-07(05)_ODP[01] software programs>*** are identified;
	CM-07(05)(b)	a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system is employed;
	CM-07(05)(c)	the list of authorized software programs is reviewed and updated ***<CM-07(05)_ODP[02] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-07(05)-Examine	[SELECT FROM: Configuration management policy; procedures addressing least functionality in the system; configuration management plan; system design documentation; system configuration settings and associated documentation; list of software programs authorized to execute on the system; system component inventory; common secure configuration checklists; review and update records associated with list of authorized software programs; change control records; system audit records; system security plan; other relevant documents or records].
	CM-07(05)-Interview	[SELECT FROM: Organizational personnel with responsibilities for identifying software authorized to execute on the system; organizational personnel with information security responsibilities; system/network administrators].
	CM-07(05)-Test	[SELECT FROM: Organizational process for identifying, reviewing, and updating programs authorized to execute on the system; organizational process for implementing authorized software policy; mechanisms supporting and/or implementing authorized software policy].

CM-07(06)	LEAST FUNCTIONALITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-07(06)_ODP	***user-installed software required to be executed in a confined environment is defined;***
	CM-07(06)	***<CM-07(06)_ODP user-installed software>*** is required to be executed in a confined physical or virtual machine environment with limited privileges.

CM-07(06)	LEAST FUNCTIONALITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-07(06)-Examine	[SELECT FROM: Configuration management policy; procedures addressing least functionality in the system; configuration management plan; system design documentation; system configuration settings and associated documentation; list or record of software required to execute in a confined environment; system component inventory; common secure configuration checklists; system audit records; system security plan; other relevant documents or records].
	CM-07(06)-Interview	[SELECT FROM: Organizational personnel with responsibilities for identifying and/or managing user-installed software and associated privileges; organizational personnel with information security responsibilities; system/network administrators].
	CM-07(06)-Test	[SELECT FROM: Organizational process for identifying user-installed software required to execute in a confined environment; mechanisms supporting and/or implementing the confinement of user-installed software to physical or virtual machine environments; mechanisms supporting and/or implementing privilege limitations on user-installed software].

CM-07(07)	LEAST FUNCTIONALITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-07(07)_ODP	***personnel or roles to explicitly approve execution of binary or machine-executable code is/are defined;***
	CM-07(07)	the execution of binary or machine-executable code is only allowed in confined physical or virtual machine environments;
	CM-07(07)(a)	the execution of binary or machine-executable code obtained from sources with limited or no warranty is only allowed with the explicit approval of ***<CM-07(07)_ODP personnel or roles>***;
	CM-07(07)(b)	the execution of binary or machine-executable code without the provision of source code is only allowed with the explicit approval of ***<CM-07(07)_ODP personnel or roles>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-07(07)-Examine	[SELECT FROM: Configuration management policy; procedures addressing least functionality in the system; configuration management plan; system design documentation; system configuration settings and associated documentation; list or record of binary or machine-executable code; system component inventory; common secure configuration checklists; system audit records; system security plan; other relevant documents or records].
	CM-07(07)-Interview	[SELECT FROM: Organizational personnel with responsibilities for approving execution of binary or machine-executable code; organizational personnel with information security responsibilities; organizational personnel with software management responsibilities; system/network administrators; system developers].

CM-07(07)	LEAST FUNCTIONALITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS	
	CM-07(07)-Test	[SELECT FROM: Organizational process for approving execution of binary or machine-executable code; organizational process for confining binary or machine-executable code to physical or virtual machine environments; mechanisms supporting and/or implementing the confinement of binary or machine-executable code to physical or virtual machine environments].

CM-07(08)	LEAST FUNCTIONALITY | BINARY OR MACHINE EXECUTABLE CODE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-07(08)(a)	the use of binary or machine-executable code is prohibited when it originates from sources with limited or no warranty or without the provision of source code;
	CM-07(08)(b)[01]	exceptions to the prohibition of binary or machine-executable code from sources with limited or no warranty or without the provision of source code are allowed only for compelling mission or operational requirements;
	CM-07(08)(b)[02]	exceptions to the prohibition of binary or machine-executable code from sources with limited or no warranty or without the provision of source code are allowed only with the approval of the authorizing official.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-07(08)-Examine	[SELECT FROM: Configuration management policy; procedures addressing least functionality in the system; configuration management plan; system security plan; system design documentation; system configuration settings and associated documentation; list or record of binary or machine-executable code; system component inventory; common secure configuration checklists; system audit records; system security plan; other relevant documents or records].
	CM-07(08)-Interview	[SELECT FROM: Organizational personnel with responsibilities for determining mission and operational requirements; authorizing official for the system; organizational personnel with information security responsibilities; organizational personnel with software management responsibilities; system/network administrators].
	CM-07(08)-Test	[SELECT FROM: Organizational process for approving execution of binary or machine-executable code; mechanisms supporting and/or implementing the prohibition of binary or machine-executable code].

CM-07(09)	LEAST FUNCTIONALITY | PROHIBITING THE USE OF UNAUTHORIZED HARDWARE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-07(09)_ODP[01]	***hardware components authorized for system use are defined;***
	CM-07(09)_ODP[02]	***frequency at which to review and update the list of authorized hardware components is defined;***
	CM-07(09)(a)	***<CM-07(09)_ODP[01] hardware components>*** are identified;
	CM-07(09)(b)	the use or connection of unauthorized hardware components is prohibited;

CM-07(09)	LEAST FUNCTIONALITY | PROHIBITING THE USE OF UNAUTHORIZED HARDWARE	
	CM-07(09)(c)	the list of authorized hardware components is reviewed and updated ***<CM-07(09)_ODP[02] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-07(09)-Examine	[SELECT FROM: Configuration management policy; network connection policy and procedures; configuration management plan; system security plan; system design documentation; system component inventory; system audit records; system security plan; other relevant documents or records].
	CM-07(09)-Interview	[SELECT FROM: Organizational personnel with system hardware management responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	CM-07(09)-Test	[SELECT FROM: Organizational process for approving execution of binary or machine-executable code; mechanisms supporting and/or implementing the prohibition of binary or machine-executable code].

CM-08	SYSTEM COMPONENT INVENTORY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-08_ODP[01]	***information deemed necessary to achieve effective system component accountability is defined;***
	CM-08_ODP[02]	***frequency at which to review and update the system component inventory is defined;***
	CM-08a.01	an inventory of system components that accurately reflects the system is developed and documented;
	CM-08a.02	an inventory of system components that includes all components within the system is developed and documented;
	CM-08a.03	an inventory of system components that does not include duplicate accounting of components or components assigned to any other system is developed and documented;
	CM-08a.04	an inventory of system components that is at the level of granularity deemed necessary for tracking and reporting is developed and documented;
	CM-08a.05	an inventory of system components that includes ***<CM-08_ODP[01] information>*** is developed and documented;
	CM-08b.	the system component inventory is reviewed and updated ***<CM-08_ODP[02] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-08-Examine	[SELECT FROM: Configuration management policy; procedures addressing system component inventory; configuration management plan; system security plan; system design documentation; system component inventory; inventory reviews and update records; system security plan; other relevant documents or records].
	CM-08-Interview	[SELECT FROM: Organizational personnel with component inventory management responsibilities; organizational personnel with information security responsibilities; system/network administrators].

CM-08	SYSTEM COMPONENT INVENTORY	
	CM-08-Test	[SELECT FROM: Organizational processes for managing the system component inventory; mechanisms supporting and/or implementing system component inventory].

CM-08(01)	SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATION AND REMOVAL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-08(01)[01]	the inventory of system components is updated as part of component installations;
	CM-08(01)[02]	the inventory of system components is updated as part of component removals;
	CM-08(01)[03]	the inventory of system components is updated as part of system updates.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-08(01)-Examine	[SELECT FROM: Configuration management policy; procedures addressing system component inventory; configuration management plan; system security plan; system component inventory; inventory reviews and update records; change control records; component installation records; component removal records; system security plan; other relevant documents or records].
	CM-08(01)-Interview	[SELECT FROM: Organizational personnel with component inventory updating responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	CM-08(01)-Test	[SELECT FROM: Organizational processes for updating the system component inventory; mechanisms supporting and/or implementing system component inventory updates].

CM-08(02)	SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-08(02)_ODP[01]	***automated mechanisms used to maintain the currency of the system component inventory are defined;***
	CM-08(02)_ODP[02]	***automated mechanisms used to maintain the completeness of the system component inventory are defined;***
	CM-08(02)_ODP[03]	***automated mechanisms used to maintain the accuracy of the system component inventory are defined;***
	CM-08(02)_ODP[04]	***automated mechanisms used to maintain the availability of the system component inventory are defined;***
	CM-08(02)[01]	***<CM-08(02)_ODP[01] automated mechanisms>*** are used to maintain the currency of the system component inventory;
	CM-08(02)[02]	***<CM-08(02)_ODP[02] automated mechanisms>*** are used to maintain the completeness of the system component inventory;

CM-08(02)	SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE	
	CM-08(02)[03]	***<CM-08(02)_ODP[03] automated mechanisms>*** are used to maintain the accuracy of the system component inventory;
	CM-08(02)[04]	***<CM-08(02)_ODP[04] automated mechanisms>*** are used to maintain the availability of the system component inventory.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-08(02)-Examine	[SELECT FROM: Configuration management policy; procedures addressing system component inventory; configuration management plan; system design documentation; system security plan; system component inventory; change control records; system maintenance records; system audit records; system security plan; other relevant documents or records].
	CM-08(02)-Interview	[SELECT FROM: Organizational personnel with component inventory management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	CM-08(02)-Test	[SELECT FROM: Organizational processes for maintaining the system component inventory; automated mechanisms supporting and/or implementing the system component inventory].

CM-08(03)	SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-08(03)_ODP[01]	***automated mechanisms used to detect the presence of unauthorized hardware within the system are defined;***
	CM-08(03)_ODP[02]	***automated mechanisms used to detect the presence of unauthorized software within the system are defined;***
	CM-08(03)_ODP[03]	***automated mechanisms used to detect the presence of unauthorized firmware within the system are defined;***
	CM-08(03)_ODP[04]	***frequency at which automated mechanisms are used to detect the presence of unauthorized system components within the system is defined;***
	CM-08(03)_ODP[05]	***one or more of the following PARAMETER VALUES is/are selected: {disable network access by unauthorized components; isolate unauthorized components; notify <CM-08(03)_ODP[06] personnel or roles>};***
	CM-08(03)_ODP[06]	***personnel or roles to be notified when unauthorized components are detected is/are defined (if selected);***
	CM-08(03)(a)[01]	the presence of unauthorized hardware within the system is detected using ***<CM-08(03)_ODP[01] automated mechanisms> <CM-08(03)_ODP[04] frequency>***;
	CM-08(03)(a)[02]	the presence of unauthorized software within the system is detected using ***<CM-08(03)_ODP[02] automated mechanisms> <CM-08(03)_ODP[04] frequency>***;
	CM-08(03)(a)[03]	the presence of unauthorized firmware within the system is detected using ***<CM-08(03)_ODP[03] automated mechanisms> <CM-08(03)_ODP[04] frequency>***;
	CM-08(03)(b)[01]	***<CM-08(03)_ODP[05] SELECTED PARAMETER VALUE(S)>*** are taken when unauthorized hardware is detected;

CM-08(03)	SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION	
	CM-08(03)(b)[02]	***<CM-08(03)_ODP[05] SELECTED PARAMETER VALUE(S)>*** are taken when unauthorized software is detected;
	CM-08(03)(b)[03]	***<CM-08(03)_ODP[05] SELECTED PARAMETER VALUE(S)>*** are taken when unauthorized firmware is detected.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-08(03)-Examine	[SELECT FROM: Configuration management policy; procedures addressing system component inventory; configuration management plan; system design documentation; system security plan; system component inventory; change control records; alerts/notifications of unauthorized components within the system; system monitoring records; system maintenance records; system audit records; system security plan; other relevant documents or records].
	CM-08(03)-Interview	[SELECT FROM: Organizational personnel with component inventory management responsibilities; organizational personnel with responsibilities for managing the automated mechanisms implementing unauthorized system component detection; organizational personnel with information security responsibilities; system/network administrators; system developers].
	CM-08(03)-Test	[SELECT FROM: Organizational processes for detection of unauthorized system components; organizational processes for taking action when unauthorized system components are detected; automated mechanisms supporting and/or implementing the detection of unauthorized system components; automated mechanisms supporting and/or implementing actions taken when unauthorized system components are detected].

CM-08(04)	SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-08(04)_ODP	***one or more of the following PARAMETER VALUES is/are selected: {name; position; role};***
	CM-08(04)	individuals responsible and accountable for administering system components are identified by ***<CM-08(04)_ODP SELECTED PARAMETER VALUE(S)>*** in the system component inventory.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-08(04)-Examine	[SELECT FROM: Configuration management policy; procedures addressing system component inventory; configuration management plan; system security plan; system component inventory; system security plan; other relevant documents or records].
	CM-08(04)-Interview	[SELECT FROM: Organizational personnel with component inventory management responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	CM-08(04)-Test	[SELECT FROM: Organizational processes for managing the system component inventory; mechanisms supporting and/or implementing the system component inventory].

CM-08(05)	SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS
	[WITHDRAWN: Incorporated into CM-08.]

CM-08(06)	SYSTEM COMPONENT INVENTORY | ASSESSED CONFIGURATIONS AND APPROVED DEVIATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-08(06)[01]	assessed component configurations are included in the system component inventory;
	CM-08(06)[02]	any approved deviations to current deployed configurations are included in the system component inventory.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-08(06)-Examine	[SELECT FROM: Configuration management policy; procedures addressing system component inventory; configuration management plan; system security plan; system design documentation; system component inventory; system configuration settings and associated documentation; change control records; system security plan; other relevant documents or records].
	CM-08(06)-Interview	[SELECT FROM: Organizational personnel with component inventory management responsibilities; organizational personnel with assessment responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	CM-08(06)-Test	[SELECT FROM: Organizational processes for managing the system component inventory; mechanisms supporting and/or implementing system component inventory].

CM-08(07)	SYSTEM COMPONENT INVENTORY | CENTRALIZED REPOSITORY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-08(07)	a centralized repository for the system component inventory is provided.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-08(07)-Examine	[SELECT FROM: Configuration management policy; procedures addressing system component inventory; configuration management plan; system design documentation; system security plan; system component inventory; system configuration settings and associated documentation; change control records; system security plan; other relevant documents or records].
	CM-08(07)-Interview	[SELECT FROM: Organizational personnel with component inventory management responsibilities; organizational personnel with security responsibilities;].
	CM-08(07)-Test	[SELECT FROM: Organizational processes for managing the system component inventory; mechanisms supporting and/or implementing system component inventory].

CM-08(08)	SYSTEM COMPONENT INVENTORY | AUTOMATED LOCATION TRACKING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-08(08)_ODP	***automated mechanisms for tracking components are defined;***
	CM-08(08)	***<CM-08(08)_ODP automated mechanisms>*** are used to support the tracking of system components by geographic location.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-08(08)-Examine	[SELECT FROM: Configuration management policy; procedures addressing system component inventory; configuration management plan; system design documentation; system component inventory; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; other relevant documents or records].
	CM-08(08)-Interview	[SELECT FROM: Organizational personnel with component inventory management responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	CM-08(08)-Test	[SELECT FROM: Organizational processes for managing the system component inventory; automated mechanisms supporting and/or implementing system component inventory; automated mechanisms supporting and/or implementing tracking of components by geographic locations].

CM-08(09)	SYSTEM COMPONENT INVENTORY | ASSIGNMENT OF COMPONENTS TO SYSTEMS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-08(09)_ODP	***personnel or roles from which to receive an acknowledgement is/are defined;***
	CM-08(09)(a)	system components are assigned to a system;
	CM-08(09)(b)	an acknowledgement of the component assignment is received from ***<CM-08(09)_ODP personnel or roles>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-08(09)-Examine	[SELECT FROM: Configuration management policy; procedures addressing system component inventory; configuration management plan; system security plan; system design documentation; system component inventory; change control records; acknowledgements of system component assignments; system security plan; other relevant documents or records].
	CM-08(09)-Interview	[SELECT FROM: Organizational personnel with component inventory management responsibilities; system owner; organizational personnel with information security responsibilities; system/network administrators].
	CM-08(09)-Test	[SELECT FROM: Organizational processes for assigning components to systems; organizational processes for acknowledging assignment of components to systems; mechanisms implementing assignment of components to the system; mechanisms implementing acknowledgment of assignment of components to the system].

CM-09	CONFIGURATION MANAGEMENT PLAN	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-09_ODP	***personnel or roles to review and approve the configuration management plan is/are defined;***
	CM-09[01]	a configuration management plan for the system is developed and documented;
	CM-09[02]	a configuration management plan for the system is implemented;
	CM-09a.[01]	the configuration management plan addresses roles;
	CM-09a.[02]	the configuration management plan addresses responsibilities;
	CM-09a.[03]	the configuration management plan addresses configuration management processes and procedures;
	CM-09b.[01]	the configuration management plan establishes a process for identifying configuration items throughout the system development life cycle;
	CM-09b.[02]	the configuration management plan establishes a process for managing the configuration of the configuration items;
	CM-09c.[01]	the configuration management plan defines the configuration items for the system;
	CM-09c.[02]	the configuration management plan places the configuration items under configuration management;
	CM-09d.	the configuration management plan is reviewed and approved by ***<CM-09_ODP personnel or roles>***;
	CM-09e.[01]	the configuration management plan is protected from unauthorized disclosure;
	CM-09e.[02]	the configuration management plan is protected from unauthorized modification.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-09-Examine	[SELECT FROM: Configuration management policy; procedures addressing configuration management planning; configuration management plan; system design documentation; system security plan; privacy plan; other relevant documents or records].
	CM-09-Interview	[SELECT FROM: Organizational personnel with responsibilities for developing the configuration management plan; organizational personnel with responsibilities for implementing and managing processes defined in the configuration management plan; organizational personnel with responsibilities for protecting the configuration management plan; organizational personnel with information security and privacy responsibilities; system/network administrators].
	CM-09-Test	[SELECT FROM: Organizational processes for developing and documenting the configuration management plan; organizational processes for identifying and managing configuration items; organizational processes for protecting the configuration management plan; mechanisms implementing the configuration management plan; mechanisms for managing configuration items; mechanisms for protecting the configuration management plan].

CM-09(01)	CONFIGURATION MANAGEMENT PLAN | ASSIGNMENT OF RESPONSIBILITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-09(01)	the responsibility for developing the configuration management process is assigned to organizational personnel who are not directly involved in system development.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-09(01)-Examine	[SELECT FROM: Configuration management policy; procedures addressing responsibilities for configuration management process development; configuration management plan; system security plan; system security plan; other relevant documents or records].
	CM-09(01)-Interview	[SELECT FROM: Organizational personnel with responsibilities for configuration management process development; organizational personnel with information security responsibilities].

CM-10	SOFTWARE USAGE RESTRICTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-10a.	software and associated documentation are used in accordance with contract agreements and copyright laws;
	CM-10b.	the use of software and associated documentation protected by quantity licenses is tracked to control copying and distribution;
	CM-10c.	the use of peer-to-peer file sharing technology is controlled and documented to ensure that peer-to-peer file sharing is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-10-Examine	[SELECT FROM: Configuration management policy; software usage restrictions; software contract agreements and copyright laws; site license documentation; list of software usage restrictions; software license tracking reports; configuration management plan; system security plan; system security plan; other relevant documents or records].
	CM-10-Interview	[SELECT FROM: Organizational personnel operating, using, and/or maintaining the system; organizational personnel with software license management responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	CM-10-Test	[SELECT FROM: Organizational processes for tracking the use of software protected by quantity licenses; organizational processes for controlling/documenting the use of peer-to-peer file sharing technology; mechanisms implementing software license tracking; mechanisms implementing and controlling the use of peer-to-peer files sharing technology].

CM-10(01)	SOFTWARE USAGE RESTRICTIONS | OPEN-SOURCE SOFTWARE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-10(01)_ODP	***restrictions on the use of open-source software are defined;***
	CM-10(01)	***<CM-10(01)_ODP restrictions>*** are established for the use of open-source software.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-10(01)-Examine	[SELECT FROM: Configuration management policy; software usage restrictions; software contract agreements and copyright laws; site license documentation; list of software usage restrictions; software license tracking reports; configuration management plan; system security plan; system security plan; other relevant documents or records].
	CM-10(01)-Interview	[SELECT FROM: Organizational personnel operating, using, and/or maintaining the system; organizational personnel with software license management responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	CM-10(01)-Test	[SELECT FROM: Organizational processes for tracking the use of software protected by quantity licenses; organizational processes for controlling/documenting the use of peer-to-peer file sharing technology; mechanisms implementing software license tracking; mechanisms implementing and controlling the use of peer-to-peer files sharing technology].

CM-11	USER-INSTALLED SOFTWARE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-11_ODP[01]	***policies governing the installation of software by users are defined;***
	CM-11_ODP[02]	***methods used to enforce software installation policies are defined;***
	CM-11_ODP[03]	***frequency with which to monitor compliance is defined;***
	CM-11a.	***<CM-11_ODP[01] policies>*** governing the installation of software by users are established;
	CM-11b.	software installation policies are enforced through ***<CM-11_ODP[02] methods>***;
	CM-11c.	compliance with ***<CM-11_ODP[01] policies>*** is monitored ***<CM-11_ODP[03] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-11-Examine	[SELECT FROM: Configuration management policy; procedures addressing user-installed software; configuration management plan; system security plan; system design documentation; system configuration settings and associated documentation; list of rules governing user installed software; system monitoring records; system audit records; continuous monitoring strategy; system security plan; other relevant documents or records].

CM-11	USER-INSTALLED SOFTWARE	
	CM-11-Interview	[SELECT FROM: Organizational personnel with responsibilities for governing user-installed software; organizational personnel operating, using, and/or maintaining the system; organizational personnel monitoring compliance with user-installed software policy; organizational personnel with information security responsibilities; system/network administrators].
	CM-11-Test	[SELECT FROM: Organizational processes governing user-installed software on the system; mechanisms enforcing policies and methods for governing the installation of software by users; mechanisms monitoring policy compliance].

CM-11(01)	USER-INSTALLED SOFTWARE | ALERTS FOR UNAUTHORIZED INSTALLATIONS	
	[WITHDRAWN: Incorporated into CM-08(03).]	

CM-11(02)	USER-INSTALLED SOFTWARE | SOFTWARE INSTALLATION WITH PRIVILEGED STATUS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-11(02)	user installation of software is allowed only with explicit privileged status.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-11(02)-Examine	[SELECT FROM: Configuration management policy; procedures addressing user-installed software; configuration management plan; system security plan; system design documentation; system configuration settings and associated documentation; alerts/notifications of unauthorized software installations; system audit records; continuous monitoring strategy; system security plan; other relevant documents or records].
	CM-11(02)-Interview	[SELECT FROM: Organizational personnel with responsibilities for governing user-installed software; organizational personnel operating, using, and/or maintaining the system; organizational personnel with information security responsibilities; system/network administrators].
	CM-11(02)-Test	[SELECT FROM: Organizational processes governing user-installed software on the system; mechanisms for prohibiting installation of software without privileged status (e.g., access controls)].

CM-11(03)	USER-INSTALLED SOFTWARE | AUTOMATED ENFORCEMENT AND MONITORING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-11(03)_ODP[01]	***automated mechanisms used to enforce compliance are defined;***
	CM-11(03)_ODP[02]	***automated mechanisms used to monitor compliance are defined;***
	CM-11(03)[01]	compliance with software installation policies is enforced using ***<CM-11(03)_ODP[01] automated mechanisms>***;

CM-11(03)	USER-INSTALLED SOFTWARE | AUTOMATED ENFORCEMENT AND MONITORING	
	CM-11(03)[02]	compliance with software installation policies is monitored using ***<CM-11(03)_ODP[02] automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-11(03)-Examine	[SELECT FROM: Configuration management policy; procedures addressing user-installed software; configuration management plan; system security plan; system design documentation; system configuration settings and associated documentation; list of rules governing user installed software; system monitoring records; system audit records; continuous monitoring strategy; system security plan; other relevant documents or records].
	CM-11(03)-Interview	[SELECT FROM: Organizational personnel with responsibilities for governing user-installed software; organizational personnel operating, using, and/or maintaining the system; organizational personnel monitoring compliance with user-installed software policy; organizational personnel with information security responsibilities; system/network administrators].
	CM-11(03)-Test	[SELECT FROM: Organizational processes governing user-installed software on the system; automated mechanisms enforcing policies on installation of software by users; automated mechanisms monitoring policy compliance].

CM-12	INFORMATION LOCATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-12_ODP	***information for which the location is to be identified and documented is defined;***
	CM-12a.[01]	the location of ***<CM-12_ODP information>*** is identified and documented;
	CM-12a.[02]	the specific system components on which ***<CM-12_ODP information>*** is processed are identified and documented;
	CM-12a.[03]	the specific system components on which ***<CM-12_ODP information>*** is stored are identified and documented;
	CM-12b.[01]	the users who have access to the system and system components where ***<CM-12_ODP information>*** is processed are identified and documented;
	CM-12b.[02]	the users who have access to the system and system components where ***<CM-12_ODP information>*** is stored are identified and documented;
	CM-12c.[01]	changes to the location (i.e., system or system components) where ***<CM-12_ODP information>*** is processed are documented;
	CM-12c.[02]	changes to the location (i.e., system or system components) where ***<CM-12_ODP information>*** is stored are documented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-12-Examine	[SELECT FROM: Configuration management policy; procedures addressing identification and documentation of information location; configuration management plan; system design documentation; system architecture documentation; PII inventory documentation; data mapping documentation; audit records; list of users with system and system component access; change control records; system component inventory; system security plan; privacy plan; other relevant documents or records].

CM-12	INFORMATION LOCATION	
	CM-12-Interview	[SELECT FROM: Organizational personnel with responsibilities for managing information location and user access to information; organizational personnel with responsibilities for operating, using, and/or maintaining the system; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	CM-12-Test	[SELECT FROM: Organizational processes governing information location; mechanisms enforcing policies and methods for governing information location].

CM-12(01)	INFORMATION LOCATION | AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-12(01)_ODP[01]	***information to be protected is defined by information type;***
	CM-12(01)_ODP[02]	***system components where the information is located are defined;***
	CM-12(01)	automated tools are used to identify ***<CM-12(01)_ODP[01] information by information type>*** on ***<CM-12(01)_ODP[02] system components>*** to ensure that controls are in place to protect organizational information and individual privacy.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-12(01)-Examine	[SELECT FROM: Configuration management policy; procedures addressing identification and documentation of information location; configuration management plan; system design documentation; PII inventory documentation; data mapping documentation; change control records; system component inventory; system security plan; privacy plan; other relevant documents or records].
	CM-12(01)-Interview	[SELECT FROM: Organizational personnel with responsibilities for managing information location; organizational personnel with information security responsibilities; system/network administrators; system developers].
	CM-12(01)-Test	[SELECT FROM: Organizational processes governing information location; automated mechanisms enforcing policies and methods for governing information location; automated tools used to identify information on system components].

CM-13	DATA ACTION MAPPING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-13	a map of system data actions is developed and documented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-13-Examine	[SELECT FROM: Configuration management policy; procedures for identification and documentation of information location; procedures for mapping data actions; configuration management plan; system security plan; privacy plan; system design documentation; PII inventory documentation; data mapping documentation; change control records; system component inventory; other relevant documents or records].

CM-13	DATA ACTION MAPPING	
	CM-13-Interview	[SELECT FROM: Organizational personnel with responsibilities for managing information location; organizational personnel responsible for data action mapping; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	CM-13-Test	[SELECT FROM: Organizational processes governing information location; mechanisms supporting or implementing data action mapping].

CM-14	SIGNED COMPONENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CM-14_ODP[01]	***software components requiring verification of a digitally signed certificate before installation are defined;***
	CM-14_ODP[02]	***firmware components requiring verification of a digitally signed certificate before installation are defined;***
	CM-14[01]	the installation of ***<CM-14_ODP[01] software components>*** is prevented unless it is verified that the software has been digitally signed using a certificate recognized and approved by the organization;
	CM-14[02]	the installation of ***<CM-14_ODP[02] firmware components>*** is prevented unless it is verified that the firmware has been digitally signed using a certificate recognized and approved by the organization.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CM-14-Examine	[SELECT FROM: Configuration management policy; procedures addressing digitally signed certificates for software and firmware components; configuration management plan; system security plan; system design documentation; change control records; system component inventory; system security plan; other relevant documents or records].
	CM-14-Interview	[SELECT FROM: Organizational personnel with responsibilities for verifying digitally signed certificates for software and firmware component installation; organizational personnel with information security responsibilities; system/network administrators; system developers].
	CM-14-Test	[SELECT FROM: Organizational processes governing information location; mechanisms enforcing policies and methods for governing information location; automated tools supporting or implementing digitally signatures for software and firmware components; automated tools supporting or implementing verification of digital signatures for software and firmware component installation].

4.6 CONTINGENCY PLANNING

CP-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-01_ODP[01]	***personnel or roles to whom the contingency planning policy is to be disseminated is/are defined;***
	CP-01_ODP[02]	***personnel or roles to whom the contingency planning procedures are to be disseminated is/are defined;***
	CP-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	CP-01_ODP[04]	***an official to manage the contingency planning policy and procedures is defined;***
	CP-01_ODP[05]	***the frequency at which the current contingency planning policy is reviewed and updated is defined;***
	CP-01_ODP[06]	***events that would require the current contingency planning policy to be reviewed and updated are defined;***
	CP-01_ODP[07]	***the frequency at which the current contingency planning procedures are reviewed and updated is defined;***
	CP-01_ODP[08]	***events that would require procedures to be reviewed and updated are defined;***
	CP-01a.[01]	a contingency planning policy is developed and documented;
	CP-01a.[02]	the contingency planning policy is disseminated to ***<CP-01_ODP[01] personnel or roles>***;
	CP-01a.[03]	contingency planning procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls are developed and documented;
	CP-01a.[04]	the contingency planning procedures are disseminated to ***<CP-01_ODP[02] personnel or roles>***;
	CP-01a.01(a)[01]	the ***<CP-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** contingency planning policy addresses purpose;
	CP-01a.01(a)[02]	the ***<CP-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** contingency planning policy addresses scope;
	CP-01a.01(a)[03]	the ***<CP-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** contingency planning policy addresses roles;
	CP-01a.01(a)[04]	the ***<CP-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** contingency planning policy addresses responsibilities;
	CP-01a.01(a)[05]	the ***<CP-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** contingency planning policy addresses management commitment;
	CP-01a.01(a)[06]	the ***<CP-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** contingency planning policy addresses coordination among organizational entities;
	CP-01a.01(a)[07]	the ***<CP-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** contingency planning policy addresses compliance;

CP-01	POLICY AND PROCEDURES	
	CP-01a.01(b)	the ***<CP-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** contingency planning policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines;
	CP-01b.	the ***<CP-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the contingency planning policy and procedures;
	CP-01c.01[01]	the current contingency planning policy is reviewed and updated ***<CP-01_ODP[05] frequency>***;
	CP-01c.01[02]	the current contingency planning policy is reviewed and updated following ***<CP-01_ODP[06] events>***;
	CP-01c.02[01]	the current contingency planning procedures are reviewed and updated ***<CP-01_ODP[07] frequency>***;
	CP-01c.02[02]	the current contingency planning procedures are reviewed and updated following ***<CP-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-01-Examine	[SELECT FROM: Contingency planning policy and procedures; system security plan; privacy plan; other relevant documents or records].
	CP-01-Interview	[SELECT FROM: Organizational personnel with contingency planning responsibilities; organizational personnel with information security and privacy responsibilities].

CP-02	CONTINGENCY PLAN	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-02_ODP[01]	***personnel or roles to review a contingency plan is/are defined;***
	CP-02_ODP[02]	***personnel or roles to approve a contingency plan is/are defined;***
	CP-02_ODP[03]	***key contingency personnel (identified by name and/or by role) to whom copies of the contingency plan are distributed are defined;***
	CP-02_ODP[04]	***key contingency organizational elements to which copies of the contingency plan are distributed are defined;***
	CP-02_ODP[05]	***frequency of contingency plan review is defined;***
	CP-02_ODP[06]	***key contingency personnel (identified by name and/or by role) to communicate changes to are defined;***
	CP-02_ODP[07]	***key contingency organizational elements to communicate changes to are defined;***
	CP-02a.01	a contingency plan for the system is developed that identifies essential mission and business functions and associated contingency requirements;
	CP-02a.02[01]	a contingency plan for the system is developed that provides recovery objectives;
	CP-02a.02[02]	a contingency plan for the system is developed that provides restoration priorities;
	CP-02a.02[03]	a contingency plan for the system is developed that provides metrics;

CP-02	CONTINGENCY PLAN	
	CP-02a.03[01]	a contingency plan for the system is developed that addresses contingency roles;
	CP-02a.03[02]	a contingency plan for the system is developed that addresses contingency responsibilities;
	CP-02a.03[03]	a contingency plan for the system is developed that addresses assigned individuals with contact information;
	CP-02a.04	a contingency plan for the system is developed that addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
	CP-02a.05	a contingency plan for the system is developed that addresses eventual, full-system restoration without deterioration of the controls originally planned and implemented;
	CP-02a.06	a contingency plan for the system is developed that addresses the sharing of contingency information;
	CP-02a.07[01]	a contingency plan for the system is developed that is reviewed by ***<CP-02_ODP[01] personnel or roles>***;
	CP-02a.07[02]	a contingency plan for the system is developed that is approved by ***<CP-02_ODP[02] personnel or roles>***;
	CP-02b.[01]	copies of the contingency plan are distributed to ***<CP-02_ODP[03] key contingency personnel>***;
	CP-02b.[02]	copies of the contingency plan are distributed to ***<CP-02_ODP[04] organizational elements>***;
	CP-02c.	contingency planning activities are coordinated with incident handling activities;
	CP-02d.	the contingency plan for the system is reviewed ***<CP-02_ODP[05] frequency>***;
	CP-02e.[01]	the contingency plan is updated to address changes to the organization, system, or environment of operation;
	CP-02e.[02]	the contingency plan is updated to address problems encountered during contingency plan implementation, execution, or testing;
	CP-02f.[01]	contingency plan changes are communicated to ***<CP-02_ODP[06] key contingency personnel>***;
	CP-02f.[02]	contingency plan changes are communicated to ***<CP-02_ODP[07] organizational elements>***;
	CP-02g.[01]	lessons learned from contingency plan testing or actual contingency activities are incorporated into contingency testing;
	CP-02g.[02]	lessons learned from contingency plan training or actual contingency activities are incorporated into contingency testing and training;
	CP-02h.[01]	the contingency plan is protected from unauthorized disclosure;
	CP-02h.[02]	the contingency plan is protected from unauthorized modification.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-02-Examine	[SELECT FROM: Contingency planning policy; procedures addressing contingency operations for the system; contingency plan; evidence of contingency plan reviews and updates; system security plan; other relevant documents or records].

CP-02	CONTINGENCY PLAN	
	CP-02-Interview	[SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with incident handling responsibilities; organizational personnel with knowledge of requirements for mission and business functions; organizational personnel with information security responsibilities].
	CP-02-Test	[SELECT FROM: Organizational processes for contingency plan development, review, update, and protection; mechanisms for developing, reviewing, updating, and/or protecting the contingency plan].

CP-02(01)	CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-02(01)	contingency plan development is coordinated with organizational elements responsible for related plans.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-02(01)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing contingency operations for the system; contingency plan; business contingency plans; disaster recovery plans; continuity of operations plans; crisis communications plans; critical infrastructure plans; cyber incident response plan; insider threat implementation plans; occupant emergency plans; system security plan; other relevant documents or records].
	CP-02(01)-Interview	[SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with information security responsibilities; personnel with responsibility for related plans].

CP-02(02)	CONTINGENCY PLAN | CAPACITY PLANNING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-02(02)[01]	capacity planning is conducted so that the necessary capacity exists during contingency operations for information processing;
	CP-02(02)[02]	capacity planning is conducted so that the necessary capacity exists during contingency operations for telecommunications;
	CP-02(02)[03]	capacity planning is conducted so that the necessary capacity exists during contingency operations for environmental support.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-02(02)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing contingency operations for the system; contingency plan; capacity planning documents; system security plan; other relevant documents or records].

CP-02(02)	CONTINGENCY PLAN | CAPACITY PLANNING	
	CP-02(02)-Interview	[SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel responsible for capacity planning; organizational personnel with information security responsibilities].

CP-02(03)	CONTINGENCY PLAN | RESUME MISSION AND BUSINESS FUNCTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-02(03)_ODP[01]	***one of the following PARAMETER VALUES is selected: {all; essential};***
	CP-02(03)_ODP[02]	***the contingency plan activation time period within which to resume mission and business functions is defined;***
	CP-02(03)	the resumption of ***<CP-02(03)_ODP[01] SELECTED PARAMETER VALUE>*** mission and business functions are planned for within ***<CP-02(03)_ODP[02] time period>*** of contingency plan activation.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-02(03)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing contingency operations for the system; contingency plan; business impact assessment; system security plan; privacy plan; other related plans; system security plan; other relevant documents or records].
	CP-02(03)-Interview	[SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with knowledge of requirements for mission and business functions].
	CP-02(03)-Test	[SELECT FROM: Organizational processes for resumption of missions and business functions].

CP-02(04)	CONTINGENCY PLAN | RESUME ALL MISSION AND BUSINESS FUNCTIONS
	[WITHDRAWN: Incorporated into CP-02(03).]

CP-02(05)	CONTINGENCY PLAN | CONTINUE MISSION AND BUSINESS FUNCTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-02(05)_ODP	***one of the following PARAMETER VALUES is selected: {all; essential};***
	CP-02(05)[01]	the continuance of ***<CP-02(05)_ODP SELECTED PARAMETER VALUE>*** mission and business functions with minimal or no loss of operational continuity is planned for;
	CP-02(05)[02]	continuity is sustained until full system restoration at primary processing and/or storage sites.

CP-02(05)	CONTINGENCY PLAN | CONTINUE MISSION AND BUSINESS FUNCTIONS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-02(05)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing contingency operations for the system; contingency plan; business impact assessment; primary processing site agreements; primary storage site agreements; alternate processing site agreements; alternate storage site agreements; contingency plan test documentation; contingency plan test results; system security plan; other relevant documents or records].
	CP-02(05)-Interview	[SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with knowledge of requirements for mission and business functions; organizational personnel with information security responsibilities].
	CP-02(05)-Test	[SELECT FROM: Organizational processes for continuing missions and business functions].

CP-02(06)	CONTINGENCY PLAN | ALTERNATE PROCESSING AND STORAGE SITES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-02(06)_ODP	***one of the following PARAMETER VALUES is selected: {all; essential};***
	CP-02(06)[01]	the transfer of ***<CP-02(06)_ODP SELECTED PARAMETER VALUE>*** mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity is planned for;
	CP-02(06)[02]	operational continuity is sustained until full system restoration at primary processing and/or storage sites.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-02(06)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing contingency operations for the system; contingency plan; business impact assessment; alternate processing site agreements; alternate storage site agreements; contingency plan testing documentation; contingency plan test results; system security plan; other relevant documents or records].
	CP-02(06)-Interview	[SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with knowledge of requirements for mission and business functions; organizational personnel with information security responsibilities].
	CP-02(06)-Test	[SELECT FROM: Organizational processes for transfer of essential mission and business functions to alternate processing/storage sites].

CP-02(07)	CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-02(07)	the contingency plan is coordinated with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.

CP-02(07)	CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-02(07)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing contingency operations for the system; contingency plan; contingency plans of external; service providers; service level agreements; contingency plan requirements; system security plan; other relevant documents or records].
	CP-02(07)-Interview	[SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities; external service providers; organizational personnel with information security responsibilities].

CP-02(08)	CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-02(08)_ODP	***one of the following PARAMETER VALUES is selected: {all; essential};***
	CP-02(08)	critical system assets supporting ***<CP-02(08)_ODP SELECTED PARAMETER VALUE>*** mission and business functions are identified.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-02(08)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing contingency operations for the system; contingency plan; business impact assessment; system security plan; other relevant documents or records].
	CP-02(08)-Interview	[SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with knowledge of requirements for mission and business functions; organizational personnel with information security responsibilities].

CP-03	CONTINGENCY TRAINING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-03_ODP[01]	***the time period within which to provide contingency training after assuming a contingency role or responsibility is defined;***
	CP-03_ODP[02]	***frequency at which to provide training to system users with a contingency role or responsibility is defined;***
	CP-03_ODP[03]	***frequency at which to review and update contingency training content is defined;***
	CP-03_ODP[04]	***events necessitating review and update of contingency training are defined;***
	CP-03a.01	contingency training is provided to system users consistent with assigned roles and responsibilities within ***<CP-03_ODP[01] time period>*** of assuming a contingency role or responsibility;
	CP-03a.02	contingency training is provided to system users consistent with assigned roles and responsibilities when required by system changes;

CP-03	CONTINGENCY TRAINING	
	CP-03a.03	contingency training is provided to system users consistent with assigned roles and responsibilities ***<CP-03_ODP[02] frequency>*** thereafter;
	CP-03b.[01]	the contingency plan training content is reviewed and updated ***<CP-03_ODP[03] frequency>***;
	CP-03b.[02]	the contingency plan training content is reviewed and updated following ***<CP-03_ODP[04] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-03-Examine	[SELECT FROM: Contingency planning policy; procedures addressing contingency training; contingency plan; contingency training curriculum; contingency training material; contingency training records; system security plan; other relevant documents or records].
	CP-03-Interview	[SELECT FROM: Organizational personnel with contingency planning, plan implementation, and training responsibilities; organizational personnel with information security responsibilities].
	CP-03-Test	[SELECT FROM: Organizational processes for contingency training].

CP-03(01)	CONTINGENCY TRAINING | SIMULATED EVENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-03(01)	simulated events are incorporated into contingency training to facilitate effective response by personnel in crisis situations.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-03(01)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing contingency training; contingency plan; contingency training curriculum; contingency training material; system security plan; other relevant documents or records].
	CP-03(01)-Interview	[SELECT FROM: Organizational personnel with contingency planning, plan implementation, and training responsibilities; organizational personnel with information security responsibilities].
	CP-03(01)-Test	[SELECT FROM: Organizational processes for contingency training; mechanisms for simulating contingency events].

CP-03(02)	CONTINGENCY TRAINING | MECHANISMS USED IN TRAINING ENVIRONMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-03(02)	mechanisms used in operations are employed to provide a more thorough and realistic contingency training environment.

CP-03(02)	CONTINGENCY TRAINING | MECHANISMS USED IN TRAINING ENVIRONMENTS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-03(02)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing contingency training; contingency plan; contingency training curriculum; contingency training material; system security plan; other relevant documents or records].
	CP-03(02)-Interview	[SELECT FROM: Organizational personnel with contingency planning, plan implementation, and training responsibilities; organizational personnel with information security responsibilities].
	CP-03(02)-Test	[SELECT FROM: Organizational processes for contingency training; mechanisms for providing contingency training environments].

CP-04	CONTINGENCY PLAN TESTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-04_ODP[01]	***frequency of testing the contingency plan for the system is defined;***
	CP-04_ODP[02]	***tests for determining the effectiveness of the contingency plan are defined;***
	CP-04_ODP[03]	***tests for determining readiness to execute the contingency plan are defined;***
	CP-04a.[01]	the contingency plan for the system is tested ***<CP-04_ODP[01] frequency>***;
	CP-04a.[02]	***<CP-04_ODP[02] tests>*** are used to determine the effectiveness of the plan;
	CP-04a.[03]	***<CP-04_ODP[03] tests>*** are used to determine the readiness to execute the plan;
	CP-04b.	the contingency plan test results are reviewed;
	CP-04c.	corrective actions are initiated, if needed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-04-Examine	[SELECT FROM: Contingency planning policy; procedures addressing contingency plan testing; contingency plan; contingency plan test documentation; contingency plan test results; system security plan; other relevant documents or records].
	CP-04-Interview	[SELECT FROM: Organizational personnel with responsibilities for contingency plan testing, reviewing, or responding to contingency plan tests; organizational personnel with information security responsibilities].
	CP-04-Test	[SELECT FROM: Organizational processes for contingency plan testing; mechanisms supporting the contingency plan and/or contingency plan testing].

CP-04(01)	CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-04(01)	contingency plan testing is coordinated with organizational elements responsible for related plans.

CP-04(01)	CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-04(01)-Examine	[SELECT FROM: Contingency planning policy; incident response policy; procedures addressing contingency plan testing; contingency plan testing documentation; contingency plan; business continuity plans; disaster recovery plans; continuity of operations plans; crisis communications plans; critical infrastructure plans; cyber incident response plans; occupant emergency plans; system security plan; other relevant documents or records].
	CP-04(01)-Interview	[SELECT FROM: Organizational personnel with contingency plan testing responsibilities; personnel with responsibilities for related plans; organizational personnel with information security responsibilities].

CP-04(02)	CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-04(02)(a)	the contingency plan is tested at the alternate processing site to familiarize contingency personnel with the facility and available resources;
	CP-04(02)(b)	the contingency plan is tested at the alternate processing site to evaluate the capabilities of the alternate processing site to support contingency operations.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-04(02)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing contingency plan testing; contingency plan; contingency plan test documentation; contingency plan test results; alternate processing site agreements; service-level agreements; system security plan; other relevant documents or records].
	CP-04(02)-Interview	[SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with information security responsibilities].
	CP-04(02)-Test	[SELECT FROM: Organizational processes for contingency plan testing; mechanisms supporting the contingency plan and/or contingency plan testing].

CP-04(03)	CONTINGENCY PLAN TESTING | AUTOMATED TESTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-04(03)_ODP	***automated mechanisms for contingency plan testing are defined;***
	CP-04(03)	the contingency plan is tested using ***<CP-04(03)_ODP automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-04(03)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing contingency plan testing; contingency plan; automated mechanisms supporting contingency plan testing; contingency plan test documentation; contingency plan test results; system security plan; other relevant documents or records].

CP-04(03)	CONTINGENCY PLAN TESTING | AUTOMATED TESTING	
	CP-04(03)-Interview	[SELECT FROM: Organizational personnel with contingency plan testing responsibilities; organizational personnel with information security responsibilities].
	CP-04(03)-Test	[SELECT FROM: Organizational processes for contingency plan testing; automated mechanisms supporting contingency plan testing].

CP-04(04)	CONTINGENCY PLAN TESTING | FULL RECOVERY AND RECONSTITUTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-04(04)[01]	a full recovery of the system to a known state is included as part of contingency plan testing;
	CP-04(04)[02]	a full reconstitution of the system to a known state is included as part of contingency plan testing.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-04(04)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing system recovery and reconstitution; contingency plan; contingency plan test documentation; contingency plan test results; system security plan; other relevant documents or records].
	CP-04(04)-Interview	[SELECT FROM: Organizational personnel with contingency plan testing responsibilities; organizational personnel with system recovery and reconstitution responsibilities; organizational personnel with information security responsibilities].
	CP-04(04)-Test	[SELECT FROM: Organizational processes for contingency plan testing; mechanisms supporting contingency plan testing; mechanisms supporting recovery and reconstitution of the system].

CP-04(05)	CONTINGENCY PLAN TESTING | SELF-CHALLENGE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-04(05)_ODP[01]	***mechanisms employed to disrupt and adversely affect the system or system component are defined;***
	CP-04(05)_ODP[02]	***system or system component on which to apply disruption mechanisms are defined;***
	CP-04(05)	***<CP-04(05)_ODP[01] mechanisms>*** are employed to disrupt and adversely affect the ***<CP-04(05)_ODP[02] system or system component>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-04(05)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing system recovery and reconstitution; contingency plan; contingency plan test documentation; contingency plan test results; system security plan; other relevant documents or records].

CP-04(05)	CONTINGENCY PLAN TESTING | SELF-CHALLENGE	
	CP-04(05)-Interview	[SELECT FROM: Organizational personnel with contingency plan testing responsibilities; organizational personnel with system recovery and reconstitution responsibilities; organizational personnel with information security responsibilities].
	CP-04(05)-Test	[SELECT FROM: Organizational processes for contingency plan testing; mechanisms supporting contingency plan testing].

CP-05	CONTINGENCY PLAN UPDATE
	[WITHDRAWN: Incorporated into CP-02.]

CP-06	ALTERNATE STORAGE SITE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-06a.[01]	an alternate storage site is established;
	CP-06a.[02]	establishment of the alternate storage site includes necessary agreements to permit the storage and retrieval of system backup information;
	CP-06b.	the alternate storage site provides controls equivalent to that of the primary site.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-06-Examine	[SELECT FROM: Contingency planning policy; procedures addressing alternate storage sites; contingency plan; alternate storage site agreements; primary storage site agreements; system security plan; other relevant documents or records].
	CP-06-Interview	[SELECT FROM: Organizational personnel with contingency plan alternate storage site responsibilities; organizational personnel with system recovery responsibilities; organizational personnel with information security responsibilities].
	CP-06-Test	[SELECT FROM: Organizational processes for storing and retrieving system backup information at the alternate storage site; mechanisms supporting and/or implementing the storage and retrieval of system backup information at the alternate storage site].

CP-06(01)	ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-06(01)	an alternate storage site that is sufficiently separated from the primary storage site is identified to reduce susceptibility to the same threats.

CP-06(01)	ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-06(01)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing alternate storage sites; contingency plan; alternate storage site; alternate storage site agreements; primary storage site agreements; system security plan; other relevant documents or records].
	CP-06(01)-Interview	[SELECT FROM: Organizational personnel with contingency plan alternate storage site responsibilities; organizational personnel with system recovery responsibilities; organizational personnel with information security responsibilities].

CP-06(02)	ALTERNATE STORAGE SITE | RECOVERY TIME AND RECOVERY POINT OBJECTIVES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-06(02)[01]	the alternate storage site is configured to facilitate recovery operations in accordance with recovery time objectives;
	CP-06(02)[02]	the alternate storage site is configured to facilitate recovery operations in accordance with recovery point objectives.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-06(02)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing alternate storage sites; contingency plan; alternate storage site; alternate storage site agreements; alternate storage site configurations; system security plan; other relevant documents or records].
	CP-06(02)-Interview	[SELECT FROM: Organizational personnel with contingency plan testing responsibilities; organizational personnel with responsibilities for testing related plans; organizational personnel with information security responsibilities].
	CP-06(02)-Test	[SELECT FROM: Organizational processes for contingency plan testing; mechanisms supporting recovery time and point objectives].

CP-06(03)	ALTERNATE STORAGE SITE | ACCESSIBILITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-06(03)[01]	potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster are identified;
	CP-06(03)[02]	explicit mitigation actions to address identified accessibility problems are outlined.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-06(03)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing alternate storage sites; contingency plan; alternate storage site; list of potential accessibility problems to alternate storage site; mitigation actions for accessibility problems to alternate storage site; organizational risk assessments; system security plan; other relevant documents or records].

CP-06(03)	ALTERNATE STORAGE SITE | ACCESSIBILITY	
	CP-06(03)-Interview	[SELECT FROM: Organizational personnel with contingency plan alternate storage site responsibilities; organizational personnel with system recovery responsibilities; organizational personnel with information security responsibilities].

CP-07	ALTERNATE PROCESSING SITE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-07_ODP[01]	***system operations for essential mission and business functions are defined;***
	CP-07_ODP[02]	***time period consistent with recovery time and recovery point objectives is defined;***
	CP-07a.	an alternate processing site, including necessary agreements to permit the transfer and resumption of ***<CP-07_ODP[01] system operations>*** for essential mission and business functions, is established within ***<CP-07_ODP[02] time period>*** when the primary processing capabilities are unavailable;
	CP-07b.[01]	the equipment and supplies required to transfer operations are made available at the alternate processing site or if contracts are in place to support delivery to the site within ***<CP-07_ODP[02] time period>*** for transfer;
	CP-07b.[02]	the equipment and supplies required to resume operations are made available at the alternate processing site or if contracts are in place to support delivery to the site within ***<CP-07_ODP[02] time period>*** for resumption;
	CP-07c.	controls provided at the alternate processing site are equivalent to those at the primary site.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-07-Examine	[SELECT FROM: Contingency planning policy; procedures addressing alternate processing sites; contingency plan; alternate processing site agreements; primary processing site agreements; spare equipment and supplies inventory at alternate processing site; equipment and supply contracts; service-level agreements; system security plan; other relevant documents or records].
	CP-07-Interview	[SELECT FROM: Organizational personnel with responsibilities for contingency planning and/or alternate site arrangements; organizational personnel with information security responsibilities].
	CP-07-Test	[SELECT FROM: Organizational processes for recovery at the alternate site; mechanisms supporting and/or implementing recovery at the alternate processing site].

CP-07(01)	ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-07(01)	an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats is identified.

CP-07(01)	ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-07(01)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing alternate processing sites; contingency plan; alternate processing site; alternate processing site agreements; primary processing site agreements; system security plan; other relevant documents or records].
	CP-07(01)-Interview	[SELECT FROM: Organizational personnel with contingency plan alternate processing site responsibilities; organizational personnel with system recovery responsibilities; organizational personnel with information security responsibilities].

CP-07(02)	ALTERNATE PROCESSING SITE | ACCESSIBILITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-07(02)[01]	potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster are identified;
	CP-07(02)[02]	explicit mitigation actions to address identified accessibility problems are outlined.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-07(02)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing alternate processing sites; contingency plan; alternate processing site; alternate processing site agreements; primary processing site agreements; system security plan; other relevant documents or records].
	CP-07(02)-Interview	[SELECT FROM: Organizational personnel with contingency plan alternate processing site responsibilities; organizational personnel with system recovery responsibilities; organizational personnel with information security responsibilities].

CP-07(03)	ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-07(03)	alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives) are developed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-07(03)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing alternate processing sites; contingency plan; alternate processing site agreements; service-level agreements; system security plan; other relevant documents or records].

CP-07(03)	ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE	
	CP-07(03)-Interview	[SELECT FROM: Organizational personnel with contingency plan alternate processing site responsibilities; organizational personnel with system recovery responsibilities; organizational personnel with information security responsibilities; organizational personnel with responsibility for acquisitions/contractual agreements].

CP-07(04)	ALTERNATE PROCESSING SITE | PREPARATION FOR USE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-07(04)	the alternate processing site is prepared so that the site can serve as the operational site supporting essential mission and business functions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-07(04)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing alternate processing sites; contingency plan; alternate processing site; alternate processing site agreements; alternate processing site configurations; system security plan; other relevant documents or records].
	CP-07(04)-Interview	[SELECT FROM: Organizational personnel with contingency plan alternate processing site responsibilities; organizational personnel with system recovery responsibilities; organizational personnel with information security responsibilities].
	CP-07(04)-Test	[SELECT FROM: Mechanisms supporting and/or implementing recovery at the alternate processing site].

CP-07(05)	ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS	
	[WITHDRAWN: Incorporated into CP-07.]	

CP-07(06)	ALTERNATE PROCESSING SITE | INABILITY TO RETURN TO PRIMARY SITE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-07(06)[01]	circumstances that preclude returning to the primary processing site are planned for;
	CP-07(06)[02]	circumstances that preclude returning to the primary processing site are prepared for.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-07(06)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing alternate processing sites; contingency plan; alternate processing site; alternate processing site agreements; alternate processing site configurations; system security plan; other relevant documents or records].

CP-07(06)	ALTERNATE PROCESSING SITE | INABILITY TO RETURN TO PRIMARY SITE	
	CP-07(06)-Interview	[SELECT FROM: Organizational personnel with system reconstitution responsibilities; organizational personnel with information security responsibilities].

CP-08	TELECOMMUNICATIONS SERVICES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-08_ODP[01]	***system operations to be resumed for essential mission and business functions are defined;***
	CP-08_ODP[02]	***time period within which to resume essential mission and business functions when the primary telecommunications capabilities are unavailable is defined;***
	CP-08	alternate telecommunications services, including necessary agreements to permit the resumption of ***<CP-08_ODP[01] system operations>*** , are established for essential mission and business functions within ***<CP-08_ODP[02] time period>*** when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-08-Examine	[SELECT FROM: Contingency planning policy; procedures addressing alternate telecommunications services; contingency plan; primary and alternate telecommunications service agreements; system security plan; other relevant documents or records].
	CP-08-Interview	[SELECT FROM: Organizational personnel with contingency plan telecommunications responsibilities; organizational personnel with system recovery responsibilities; organizational personnel with knowledge of requirements for mission and business functions; organizational personnel with information security responsibilities; organizational personnel with responsibility for acquisitions/ contractual agreements].
	CP-08-Test	[SELECT FROM: Mechanisms supporting telecommunications].

CP-08(01)	TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-08(01)(a)[01]	primary telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives) are developed;
	CP-08(01)(a)[02]	alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives) are developed;
	CP-08(01)(b)	Telecommunications Service Priority is requested for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

CP-08(01)	TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-08(01)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing primary and alternate telecommunications services; contingency plan; primary and alternate telecommunications service agreements; Telecommunications Service Priority documentation; system security plan; other relevant documents or records].
	CP-08(01)-Interview	[SELECT FROM: Organizational personnel with contingency plan telecommunications responsibilities; organizational personnel with system recovery responsibilities; organizational personnel with information security responsibilities; organizational personnel with responsibility for acquisitions/ contractual agreements].
	CP-08(01)-Test	[SELECT FROM: Mechanisms supporting telecommunications].

CP-08(02)	TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-08(02)	alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services are obtained.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-08(02)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing primary and alternate telecommunications services; contingency plan; primary and alternate telecommunications service agreements; system security plan; other relevant documents or records].
	CP-08(02)-Interview	[SELECT FROM: Organizational personnel with contingency plan telecommunications responsibilities; organizational personnel with system recovery responsibilities; primary and alternate telecommunications service providers; organizational personnel with information security responsibilities].

CP-08(03)	TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-08(03)	alternate telecommunications services from providers that are separated from primary service providers are obtained to reduce susceptibility to the same threats.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-08(03)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing primary and alternate telecommunications services; contingency plan; primary and alternate telecommunications service agreements; alternate telecommunications service provider site; primary telecommunications service provider site; other relevant documents or records].

CP-08(03)	TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS	
	CP-08(03)-Interview	[SELECT FROM: Organizational personnel with contingency plan telecommunications responsibilities; organizational personnel with system recovery responsibilities; primary and alternate telecommunications service providers; organizational personnel with information security responsibilities].

CP-08(04)	TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-08(04)_ODP[01]	***frequency at which to obtain evidence of contingency testing by providers is defined;***
	CP-08(04)_ODP[02]	***frequency at which to obtain evidence of contingency training by providers is defined;***
	CP-08(04)(a)[01]	primary telecommunications service providers are required to have contingency plans;
	CP-08(04)(a)[02]	alternate telecommunications service providers are required to have contingency plans;
	CP-08(04)(b)	provider contingency plans are reviewed to ensure that the plans meet organizational contingency requirements;
	CP-08(04)(c)[01]	evidence of contingency testing by providers is obtained ***<CP-08(04)_ODP[01] frequency>***.
	CP-08(04)(c)[02]	evidence of contingency training by providers is obtained ***<CP-08(04)_ODP[02] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-08(04)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing primary and alternate telecommunications services; contingency plan; provider contingency plans; evidence of contingency testing/training by providers; primary and alternate telecommunications service agreements; system security plan; other relevant documents or records].
	CP-08(04)-Interview	[SELECT FROM: Organizational personnel with contingency planning, plan implementation, and testing responsibilities; primary and alternate telecommunications service providers; organizational personnel with information security responsibilities; organizational personnel with responsibility for acquisitions/contractual agreements].

CP-08(05)	TELECOMMUNICATIONS SERVICES | ALTERNATE TELECOMMUNICATION SERVICE TESTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-08(05)_ODP	***frequency at which alternate telecommunications services are tested is defined;***
	CP-08(05)	alternate telecommunications services are tested ***<CP-08(05)_ODP frequency>***.

CP-08(05)	TELECOMMUNICATIONS SERVICES | ALTERNATE TELECOMMUNICATION SERVICE TESTING	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-08(05)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing alternate telecommunications services; contingency plan; evidence of testing alternate telecommunications services; alternate telecommunications service agreements; system security plan; other relevant documents or records].
	CP-08(05)-Interview	[SELECT FROM: Organizational personnel with contingency planning, plan implementation, and testing responsibilities; alternate telecommunications service providers; organizational personnel with information security responsibilities].
	CP-08(05)-Test	[SELECT FROM: Mechanisms supporting testing alternate telecommunications services].

CP-09	SYSTEM BACKUP	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-09_ODP[01]	***system components for which to conduct backups of user-level information is defined;***
	CP-09_ODP[02]	***frequency at which to conduct backups of user-level information consistent with recovery time and recovery point objectives is defined;***
	CP-09_ODP[03]	***frequency at which to conduct backups of system-level information consistent with recovery time and recovery point objectives is defined;***
	CP-09_ODP[04]	***frequency at which to conduct backups of system documentation consistent with recovery time and recovery point objectives is defined;***
	CP-09a.	backups of user-level information contained in ***<CP-09_ODP[01] system components>*** are conducted ***<CP-09_ODP[02] frequency>***;
	CP-09b.	backups of system-level information contained in the system are conducted ***<CP-09_ODP[03] frequency>***;
	CP-09c.	backups of system documentation, including security- and privacy-related documentation are conducted ***<CP-09_ODP[04] frequency>***;
	CP-09d.[01]	the confidentiality of backup information is protected;
	CP-09d.[02]	the integrity of backup information is protected;
	CP-09d.[03]	the availability of backup information is protected.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-09-Examine	[SELECT FROM: Contingency planning policy; procedures addressing system backup; contingency plan; backup storage location(s); system backup logs or records; system security plan; privacy plan; other relevant documents or records].
	CP-09-Interview	[SELECT FROM: Organizational personnel with system backup responsibilities; organizational personnel with information security and privacy responsibilities].
	CP-09-Test	[SELECT FROM: Organizational processes for conducting system backups; mechanisms supporting and/or implementing system backups].

CP-09(01)	SYSTEM BACKUP | TESTING FOR RELIABILITY AND INTEGRITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-09(01)_ODP[01]	***frequency at which to test backup information for media reliability is defined;***
	CP-09(01)_ODP[02]	***frequency at which to test backup information for information integrity is defined;***
	CP-09(01)[01]	backup information is tested ***<CP-09(01)_ODP[01] frequency>*** to verify media reliability;
	CP-09(01)[02]	backup information is tested ***<CP-09(01)_ODP[02] frequency>*** to verify information integrity.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-09(01)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing system backup; contingency plan; system backup test results; contingency plan test documentation; contingency plan test results; system security plan; other relevant documents or records].
	CP-09(01)-Interview	[SELECT FROM: Organizational personnel with system backup responsibilities; organizational personnel with information security responsibilities].
	CP-09(01)-Test	[SELECT FROM: Organizational processes for conducting system backups; mechanisms supporting and/or implementing system backups].

CP-09(02)	SYSTEM BACKUP | TEST RESTORATION USING SAMPLING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-09(02)	a sample of backup information in the restoration of selected system functions is used as part of contingency plan testing.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-09(02)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing system backup; contingency plan; system backup test results; contingency plan test documentation; contingency plan test results; system security plan; other relevant documents or records].
	CP-09(02)-Interview	[SELECT FROM: Organizational personnel with system backup responsibilities; organizational personnel with contingency planning/contingency plan testing responsibilities; organizational personnel with information security responsibilities].
	CP-09(02)-Test	[SELECT FROM: Organizational processes for conducting system backups; mechanisms supporting and/or implementing system backups].

CP-09(03)	SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-09(03)_ODP	***critical system software and other security-related information backups to be stored in a separate facility are defined;***
	CP-09(03)	backup copies of ***<CP-09(03)_ODP critical system software and other security-related information>*** are stored in a separate facility or in a fire rated container that is not collocated with the operational system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-09(03)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing system backup; contingency plan; backup storage location(s); system backup configurations and associated documentation; system backup logs or records; system security plan; other relevant documents or records].
	CP-09(03)-Interview	[SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with system backup responsibilities; organizational personnel with information security responsibilities].

CP-09(04)	SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION
	[WITHDRAWN: Incorporated into CP-09.]

CP-09(05)	SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-09(05)_ODP[01]	***time period consistent with recovery time and recovery point objectives is defined;***
	CP-09(05)_ODP[02]	***transfer rate consistent with recovery time and recovery point objectives is defined;***
	CP-09(05)[01]	system backup information is transferred to the alternate storage site for ***<CP-09(05)_ODP[01] time period>***;
	CP-09(05)[02]	system backup information is transferred to the alternate storage site ***<CP-09(05)_ODP[02] transfer rate>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-09(05)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing system backup; contingency plan; system backup logs or records; evidence of system backup information transferred to alternate storage site; alternate storage site agreements; system security plan; other relevant documents or records].
	CP-09(05)-Interview	[SELECT FROM: Organizational personnel with system backup responsibilities; organizational personnel with information security responsibilities].

CP-09(05)	SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE	
	CP-09(05)-Test	[SELECT FROM: Organizational processes for transferring system backups to the alternate storage site; mechanisms supporting and/or implementing system backups; mechanisms supporting and/or implementing information transfer to the alternate storage site].

CP-09(06)	SYSTEM BACKUP | REDUNDANT SECONDARY SYSTEM	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-09(06)[01]	system backup is conducted by maintaining a redundant secondary system that is not collocated with the primary system;
	CP-09(06)[02]	system backup is conducted by maintaining a redundant secondary system that can be activated without loss of information or disruption to operations.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-09(06)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing system backup; contingency plan; system backup test results; contingency plan test results; contingency plan test documentation; redundant secondary system for system backups; location(s) of redundant secondary backup system(s); system security plan; other relevant documents or records].
	CP-09(06)-Interview	[SELECT FROM: Organizational personnel with system backup responsibilities; organizational personnel with information security responsibilities; organizational personnel with responsibility for the redundant secondary system].
	CP-09(06)-Test	[SELECT FROM: Organizational processes for maintaining redundant secondary systems; mechanisms supporting and/or implementing system backups; mechanisms supporting and/or implementing information transfer to a redundant secondary system].

CP-09(07)	SYSTEM BACKUP | DUAL AUTHORIZATION FOR DELETION OR DESTRUCTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-09(07)_ODP	***backup information for which to enforce dual authorization in order to delete or destroy is defined;***
	CP-09(07)	dual authorization for the deletion or destruction of ***<CP-09(07)_ODP backup information>*** is enforced.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-09(07)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing system backup; contingency plan; system design documentation; system configuration settings and associated documentation; system generated list of dual authorization credentials or rules; logs or records of deletion or destruction of backup information; system security plan; other relevant documents or records].
	CP-09(07)-Interview	[SELECT FROM: Organizational personnel with system backup responsibilities; organizational personnel with information security responsibilities].

CP-09(07)	SYSTEM BACKUP | DUAL AUTHORIZATION FOR DELETION OR DESTRUCTION	
	CP-09(07)-Test	[SELECT FROM: Mechanisms supporting and/or implementing dual authorization; mechanisms supporting and/or implementing the deletion/destruction of backup information].

CP-09(08)	SYSTEM BACKUP | CRYPTOGRAPHIC PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-09(08)_ODP	***backup information to protect against unauthorized disclosure and modification is defined;***
	CP-09(08)	cryptographic mechanisms are implemented to prevent unauthorized disclosure and modification of ***<CP-09(08)_ODP backup information>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-09(08)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing system backup; contingency plan; system design documentation; system configuration settings and associated documentation; system security plan; other relevant documents or records].
	CP-09(08)-Interview	[SELECT FROM: Organizational personnel with system backup responsibilities; organizational personnel with information security responsibilities].
	CP-09(08)-Test	[SELECT FROM: Mechanisms supporting and/or implementing cryptographic protection of backup information].

CP-10	SYSTEM RECOVERY AND RECONSTITUTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-10_ODP[01]	***time period consistent with recovery time and recovery point objectives for the recovery of the system is determined;***
	CP-10_ODP[02]	***time period consistent with recovery time and recovery point objectives for the reconstitution of the system is determined;***
	CP-10[01]	the recovery of the system to a known state is provided within ***<CP-10_ODP[01] time period>*** after a disruption, compromise, or failure;
	CP-10[02]	a reconstitution of the system to a known state is provided within ***<CP-10_ODP[02] time period>*** after a disruption, compromise, or failure.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-10-Examine	[SELECT FROM: Contingency planning policy; procedures addressing system backup; contingency plan; system backup test results; contingency plan test results; contingency plan test documentation; redundant secondary system for system backups; location(s) of redundant secondary backup system(s); system security plan; other relevant documents or records].

CP-10	SYSTEM RECOVERY AND RECONSTITUTION	
	CP-10-Interview	[SELECT FROM: Organizational personnel with contingency planning, recovery, and/or reconstitution responsibilities; organizational personnel with information security responsibilities].
	CP-10-Test	[SELECT FROM: Organizational processes implementing system recovery and reconstitution operations; mechanisms supporting and/or implementing system recovery and reconstitution operations].

CP-10(01)	SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING	
	[WITHDRAWN: Incorporated into CP-04.]	

CP-10(02)	SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-10(02)	transaction recovery is implemented for systems that are transaction-based.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-10(02)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing system recovery and reconstitution; contingency plan; system design documentation; system configuration settings and associated documentation; contingency plan test documentation; contingency plan test results; system transaction recovery records; system audit records; system security plan; other relevant documents or records].
	CP-10(02)-Interview	[SELECT FROM: Organizational personnel with responsibility for transaction recovery; organizational personnel with information security responsibilities].
	CP-10(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing transaction recovery capability].

CP-10(03)	SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS	
	[WITHDRAWN. Addressed through tailoring.]	

CP-10(04)	SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-10(04)_ODP	***restoration time period within which to restore system components to a known, operational state is defined;***
	CP-10(04)	the capability to restore system components within ***<CP-10(04)_ODP restoration time periods>*** from configuration-controlled and integrity-protected information representing a known, operational state for the components is provided.

CP-10(04)	SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-10(04)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing system recovery and reconstitution; contingency plan; system design documentation; system configuration settings and associated documentation; contingency plan test documentation; contingency plan test results; evidence of system recovery and reconstitution operations; system security plan; other relevant documents or records].
	CP-10(04)-Interview	[SELECT FROM: Organizational personnel with system recovery and reconstitution responsibilities; organizational personnel with information security responsibilities].
	CP-10(04)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the recovery/ reconstitution of system information].

CP-10(05)	SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY
	[WITHDRAWN: Incorporated into SI-13.]

CP-10(06)	SYSTEM RECOVERY AND RECONSTITUTION | COMPONENT PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-10(06)	system components used for recovery and reconstitution are protected.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-10(06)-Examine	[SELECT FROM: Contingency planning policy; procedures addressing system recovery and reconstitution; contingency plan; system design documentation; system configuration settings and associated documentation; logical access credentials; physical access credentials; logical access authorization records; physical access authorization records; system security plan; other relevant documents or records].
	CP-10(06)-Interview	[SELECT FROM: Organizational personnel with system recovery and reconstitution responsibilities; organizational personnel with information security responsibilities].
	CP-10(06)-Test	[SELECT FROM: Organizational processes for protecting backup and restoration of hardware, firmware, and software; mechanisms supporting and/or implementing protection of backups and restoration of hardware, firmware, and software].

CP-11	ALTERNATE COMMUNICATIONS PROTOCOLS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-11_ODP	***alternative communications protocols in support of maintaining continuity of operations are defined;***

CP-11	ALTERNATE COMMUNICATIONS PROTOCOLS	
	CP-11	the capability to employ ***<CP-11_ODP alternative communications protocols>*** are provided in support of maintaining continuity of operations.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-11-Examine	[SELECT FROM: Contingency planning policy; procedures addressing alternative communications protocols; contingency plan; continuity of operations plan; system design documentation; system configuration settings and associated documentation; list of alternative communications protocols supporting continuity of operations; system security plan; other relevant documents or records].
	CP-11-Interview	[SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with continuity of operations planning and plan implementation responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	CP-11-Test	[SELECT FROM: Mechanisms employing alternative communications protocols].

CP-12	SAFE MODE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-12_ODP[01]	***restrictions for safe mode of operation are defined;***
	CP-12_ODP[02]	***conditions detected to enter a safe mode of operation are defined;***
	CP-12	a safe mode of operation is entered with ***<CP-12_ODP[01] restrictions>*** when ***<CP-12_ODP[02] conditions>*** are detected.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-12-Examine	[SELECT FROM: Contingency planning policy; procedures addressing safe mode of operation for the system; contingency plan; system design documentation; system configuration settings and associated documentation; system administration manuals; system operation manuals; system installation manuals; contingency plan test records; incident handling records; system audit records; system security plan; other relevant documents or records].
	CP-12-Interview	[SELECT FROM: Organizational personnel with system operation responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	CP-12-Test	[SELECT FROM: Mechanisms implementing safe mode of operation].

CP-13	ALTERNATIVE SECURITY MECHANISMS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	CP-13_ODP[01]	***alternative or supplemental security mechanisms are defined;***
	CP-13_ODP[02]	***security functions are defined;***

CP-13	ALTERNATIVE SECURITY MECHANISMS	
	CP-13	***<CP-13_ODP[01] alternative or supplemental security mechanisms>*** are employed for satisfying ***<CP-13_ODP[02] security functions>*** when the primary means of implementing the security function is unavailable or compromised.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	CP-13-Examine	[SELECT FROM: Contingency planning policy; procedures addressing alternate security mechanisms; contingency plan; continuity of operations plan; system design documentation; system configuration settings and associated documentation; contingency plan test records; contingency plan test results; system security plan; other relevant documents or records].
	CP-13-Interview	[SELECT FROM: Organizational personnel with system operation responsibilities; organizational personnel with information security responsibilities].
	CP-13-Test	[SELECT FROM: system capability implementing alternative security mechanisms].

4.7 IDENTIFICATION AND AUTHENTICATION

IA-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-01_ODP[01]	***personnel or roles to whom the identification and authentication policy is to be disseminated are defined;***
	IA-01_ODP[02]	***personnel or roles to whom the identification and authentication procedures are to be disseminated is/are defined;***
	IA-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	IA-01_ODP[04]	***an official to manage the identification and authentication policy and procedures is defined;***
	IA-01_ODP[05]	***the frequency at which the current identification and authentication policy is reviewed and updated is defined;***
	IA-01_ODP[06]	***events that would require the current identification and authentication policy to be reviewed and updated are defined;***
	IA-01_ODP[07]	***the frequency at which the current identification and authentication procedures are reviewed and updated is defined;***
	IA-01_ODP[08]	***events that would require identification and authentication procedures to be reviewed and updated are defined;***
	IA-01a.[01]	an identification and authentication policy is developed and documented;
	IA-01a.[02]	the identification and authentication policy is disseminated to ***<IA-01_ODP[01] personnel or roles>***;
	IA-01a.[03]	identification and authentication procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls are developed and documented;
	IA-01a.[04]	the identification and authentication procedures are disseminated to ***<IA-01_ODP[02] personnel or roles>***;
	IA-01a.01(a)[01]	the ***<IA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** identification and authentication policy addresses purpose;
	IA-01a.01(a)[02]	the ***<IA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** identification and authentication policy addresses scope;
	IA-01a.01(a)[03]	the ***<IA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** identification and authentication policy addresses roles;
	IA-01a.01(a)[04]	the ***<IA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** identification and authentication policy addresses responsibilities;
	IA-01a.01(a)[05]	the ***<IA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** identification and authentication policy addresses management commitment;
	IA-01a.01(a)[06]	the ***<IA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** identification and authentication policy addresses coordination among organizational entities;

IA-01	POLICY AND PROCEDURES	
	IA-01a.01(a)[07]	the ***<IA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** identification and authentication policy addresses compliance;
	IA-01a.01(b)	the ***<IA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** identification and authentication policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines;
	IA-01b.	the ***<IA-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the identification and authentication policy and procedures;
	IA-01c.01[01]	the current identification and authentication policy is reviewed and updated ***<IA-01_ODP[05] frequency>***;
	IA-01c.01[02]	the current identification and authentication policy is reviewed and updated following ***<IA-01_ODP[06] events>***;
	IA-01c.02[01]	the current identification and authentication procedures are reviewed and updated ***<IA-01_ODP[07] frequency>***;
	IA-01c.02[02]	the current identification and authentication procedures are reviewed and updated following ***<IA-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-01-Examine	[SELECT FROM: Identification and authentication policy and procedures; system security plan; privacy plan; risk management strategy documentation; list of events requiring identification and authentication procedures to be reviewed and updated (e.g., audit findings); other relevant documents or records].
	IA-01-Interview	[SELECT FROM: Organizational personnel with identification and authentication responsibilities; organizational personnel with information security and privacy responsibilities].

IA-02	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-02[01]	organizational users are uniquely identified and authenticated;
	IA-02[02]	the unique identification of authenticated organizational users is associated with processes acting on behalf of those users.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-02-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing user identification and authentication; system security plan, system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records].
	IA-02-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/ network administrators; organizational personnel with account management responsibilities; system developers].

IA-02	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	
	IA-02-Test	[SELECT FROM: Organizational processes for uniquely identifying and authenticating users; mechanisms supporting and/or implementing identification and authentication capabilities].

IA-02(01)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-02(01)	multi-factor authentication is implemented for access to privileged accounts.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-02(01)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing user identification and authentication; system security plan; system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records].
	IA-02(01)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-02(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing a multi-factor authentication capability].

IA-02(02)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-02(02)	multi-factor authentication for access to non-privileged accounts is implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-02(02)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records].
	IA-02(02)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-02(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing a multi-factor authentication capability].

IA-02(03)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO PRIVILEGED ACCOUNTS
	[WITHDRAWN: Incorporated into IA-02(01).]

IA-02(04)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS
	[WITHDRAWN: Incorporated into IA-02(02).]

IA-02(05)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | INDIVIDUAL AUTHENTICATION WITH GROUP AUTHENTICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-02(05)	users are required to be individually authenticated before granting access to the shared accounts or resources when shared accounts or authenticators are employed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-02(05)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records].
	IA-02(05)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-02(05)-Test	[SELECT FROM: Mechanisms supporting and/or implementing an authentication capability for group accounts].

IA-02(06)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCESS TO ACCOUNTS —SEPARATE DEVICE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-02(06)_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {local; network; remote};***
	IA-02(06)_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {privileged accounts; non-privileged accounts};***
	IA-02(06)_ODP[03]	***the strength of mechanism requirements to be enforced by a device separate from the system gaining access to accounts is defined;***

IA-02(06)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCESS TO ACCOUNTS —SEPARATE DEVICE	
	IA-02(06)(a)	multi-factor authentication is implemented for ***<IA-02(06)_ODP[01] SELECTED PARAMETER VALUE(S)>*** access to ***<IA-02(06)_ODP[02] SELECTED PARAMETER VALUE(S)>*** such that one of the factors is provided by a device separate from the system gaining access;
	IA-02(06)(b)	multi-factor authentication is implemented for ***<IA-02(06)_ODP[01] SELECTED PARAMETER VALUE(S)>*** access to ***<IA-02(06)_ODP[02] SELECTED PARAMETER VALUE(S)>*** such that the device meets ***<IA-02(06)_ODP[03] strength of mechanism requirements>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-02(06)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records].
	IA-02(06)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-02(06)-Test	[SELECT FROM: Mechanisms supporting and/or implementing multi-factor authentication capability].

IA-02(07)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — SEPARATE DEVICE	
	[WITHDRAWN: Incorporated into IA-02(06).]	

IA-02(08)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCESS TO ACCOUNTS — REPLAY RESISTANT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-02(08)_ODP	***one or more of the following PARAMETER VALUES is/are selected: {privileged accounts; non-privileged accounts};***
	IA-02(08)	replay-resistant authentication mechanisms for access to ***<IA-02(08)_ODP SELECTED PARAMETER VALUE(S)>*** are implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-02(08)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; list of privileged system accounts; other relevant documents or records].

IA-02(08)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCESS TO ACCOUNTS — REPLAY RESISTANT	
	IA-02(08)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-02(08)-Test	[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities; Mechanisms supporting and/or implementing replay-resistant authentication mechanisms].

IA-02(09)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — REPLAY RESISTANT	
	[WITHDRAWN: Incorporated into IA-02(08).]	

IA-02(10)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | SINGLE SIGN-ON	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-02(10)_ODP	***system accounts and services for which a single sign-on capability must be provided are defined;***
	IA-02(10)	a single sign-on capability is provided for ***<IA-02(10)_ODP system accounts and services>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-02(10)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing single sign-on capability for system accounts and services; procedures addressing identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts and services requiring single sign-on capability; other relevant documents or records].
	IA-02(10)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-02(10)-Test	[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities; mechanisms supporting and/or implementing single sign-on capability for system accounts and services].

IA-02(11)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | REMOTE ACCESS — SEPARATE DEVICE	
	[WITHDRAWN: Incorporated into IA-02(06).]	

IA-02(12)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-02(12)	Personal Identity Verification-compliant credentials are accepted and electronically verified.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-02(12)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; PIV verification records; evidence of PIV credentials; PIV credential authorizations; other relevant documents or records].
	IA-02(12)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-02(12)-Test	[SELECT FROM: Mechanisms supporting and/or implementing acceptance and verification of PIV credentials].

IA-02(13)	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | OUT-OF-BAND AUTHENTICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-02(13)_ODP[01]	***out-of-band authentication mechanisms to be implemented are defined;***
	IA-02(13)_ODP[02]	***conditions under which out-of-band authentication is to be implemented are defined;***
	IA-02(13)	***<IA-02(13)_ODP[01] out-of-band authentication>*** mechanisms are implemented under ***<IA-02(13)_ODP[02] conditions>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-02(13)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; system-generated list of out-of-band authentication paths; other relevant documents or records].
	IA-02(13)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-02(13)-Test	[SELECT FROM: Mechanisms supporting and/or implementing out-of-band authentication capability].

IA-03	DEVICE IDENTIFICATION AND AUTHENTICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-03_ODP[01]	***devices and/or types of devices to be uniquely identified and authenticated before establishing a connection are defined;***
	IA-03_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {local; remote; network};***
	IA-03	***<IA-03_ODP[01] devices and/or types of devices>*** are uniquely identified and authenticated before establishing a ***<IA-03_ODP[02] SELECTED PARAMETER VALUE(S)>*** connection.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-03-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing device identification and authentication; system design documentation; list of devices requiring unique identification and authentication; device connection reports; system configuration settings and associated documentation; other relevant documents or records].
	IA-03-Interview	[SELECT FROM: Organizational personnel with operational responsibilities for device identification and authentication; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-03-Test	[SELECT FROM: Mechanisms supporting and/or implementing device identification and authentication capabilities].

IA-03(01)	DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-03(01)_ODP[01]	***devices and/or types of devices requiring use of cryptographically based, bidirectional authentication to authenticate before establishing one or more connections are defined;***
	IA-03(01)_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {local; remote; network};***
	IA-03(01)	***<IA-03(01)_ODP[01] devices and/or types of devices>*** are authenticated before establishing ***<IA-03(01)_ODP[02] SELECTED PARAMETER VALUE(S)>*** connection using bidirectional authentication that is cryptographically based.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-03(01)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing device identification and authentication; system design documentation; list of devices requiring unique identification and authentication; device connection reports; system configuration settings and associated documentation; other relevant documents or records].
	IA-03(01)-Interview	[SELECT FROM: Organizational personnel with operational responsibilities for device identification and authentication; organizational personnel with information security responsibilities; system/network administrators; system developers].

IA-03(01)	DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION	
	IA-03(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing device authentication capability; cryptographically based bidirectional authentication mechanisms].

IA-03(02)	DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION	
	[WITHDRAWN: Incorporated into IA-03(01).]	

IA-03(03)	DEVICE IDENTIFICATION AND AUTHENTICATION | DYNAMIC ADDRESS ALLOCATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-03(03)_ODP[01]	***lease information to be employed to standardize dynamic address allocation for devices is defined;***
	IA-03(03)_ODP[02]	***lease duration to be employed to standardize dynamic address allocation for devices is defined;***
	IA-03(03)(a)[01]	dynamic address allocation lease information assigned to devices where addresses are allocated dynamically are standardized in accordance with ***<IA-03(03)_ODP[01] lease information>***;
	IA-03(03)(a)[02]	dynamic address allocation lease duration assigned to devices where addresses are allocated dynamically are standardized in accordance with ***<IA-03(03)_ODP[02] lease duration>***;
	IA-03(03)(b)	lease information is audited when assigned to a device.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-03(03)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing device identification and authentication; system design documentation; system configuration settings and associated documentation; evidence of lease information and lease duration assigned to devices; device connection reports; system audit records; other relevant documents or records].
	IA-03(03)-Interview	[SELECT FROM: Organizational personnel with operational responsibilities for device identification and authentication; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-03(03)-Test	[SELECT FROM: Mechanisms supporting and/or implementing device identification and authentication capabilities; mechanisms supporting and/or implementing dynamic address allocation; mechanisms supporting and/or implanting auditing of lease information].

IA-03(04)	DEVICE IDENTIFICATION AND AUTHENTICATION | DEVICE ATTESTATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-03(04)_ODP	***configuration management process to be employed to handle device identification and authentication based on attestation is defined;***
	IA-03(04)	device identification and authentication are handled based on attestation by ***<IA-03(04)_ODP configuration management process>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-03(04)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing device identification and authentication; procedures addressing device configuration management; system design documentation; system configuration settings and associated documentation; configuration management records; change control records; system audit records; other relevant documents or records].
	IA-03(04)-Interview	[SELECT FROM: Organizational personnel with operational responsibilities for device identification and authentication; organizational personnel with information security responsibilities; system/network administrators].
	IA-03(04)-Test	[SELECT FROM: Mechanisms supporting and/or implementing device identification and authentication capabilities; mechanisms supporting and/or implementing configuration management; cryptographic mechanisms supporting device attestation].

IA-04	IDENTIFIER MANAGEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-04_ODP[01]	***personnel or roles from whom authorization must be received to assign an identifier are defined;***
	IA-04_ODP[02]	***a time period for preventing reuse of identifiers is defined;***
	IA-04a.	system identifiers are managed by receiving authorization from ***<IA-04_ODP[01] personnel or roles>*** to assign to an individual, group, role, or device identifier;
	IA-04b.	system identifiers are managed by selecting an identifier that identifies an individual, group, role, service, or device;
	IA-04c.	system identifiers are managed by assigning the identifier to the intended individual, group, role, service, or device;
	IA-04d.	system identifiers are managed by preventing reuse of identifiers for ***<IA-04_ODP[02] time period>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-04-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of system accounts; list of identifiers generated from physical access control devices; other relevant documents or records].

IA-04	IDENTIFIER MANAGEMENT	
	IA-04-Interview	[SELECT FROM: Organizational personnel with identifier management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-04-Test	[SELECT FROM: Mechanisms supporting and/or implementing identifier management].

IA-04(01)	IDENTIFIER MANAGEMENT | PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-04(01)	the use of system account identifiers that are the same as public identifiers is prohibited for individual accounts.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-04(01)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing identifier management; procedures addressing account management; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	IA-04(01)-Interview	[SELECT FROM: Organizational personnel with identifier management responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	IA-04(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing identifier management].

IA-04(02)	IDENTIFIER MANAGEMENT | SUPERVISOR AUTHORIZATION
	[WITHDRAWN: Incorporated into IA-12(01).]

IA-04(03)	IDENTIFIER MANAGEMENT | MULTIPLE FORMS OF CERTIFICATION
	[WITHDRAWN: Incorporated into IA-12(02).]

IA-04(04)	IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-04(04)_ODP	***characteristics used to identify individual status is defined;***
	IA-04(04)	individual identifiers are managed by uniquely identifying each individual as ***<IA-04(04)_ODP characteristics>***.

IA-04(04)	IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-04(04)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing identifier management; procedures addressing account management; list of characteristics identifying individual status; other relevant documents or records].
	IA-04(04)-Interview	[SELECT FROM: Organizational personnel with identifier management responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	IA-04(04)-Test	[SELECT FROM: Mechanisms supporting and/or implementing identifier management].

IA-04(05)	IDENTIFIER MANAGEMENT | DYNAMIC MANAGEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-04(05)_ODP	***a dynamic identifier policy for managing individual identifiers is defined;***
	IA-04(05)	individual identifiers are dynamically managed in accordance with ***<IA-04(05)_ODP dynamic identifier policy>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-04(05)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing identifier management; procedures addressing account management; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	IA-04(05)-Interview	[SELECT FROM: Organizational personnel with identifier management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-04(05)-Test	[SELECT FROM: Mechanisms supporting and/or implementing dynamic identifier management].

IA-04(06)	IDENTIFIER MANAGEMENT | CROSS-ORGANIZATION MANAGEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-04(06)_ODP	***external organizations with whom to coordinate the cross-organization management of identifiers are defined;***
	IA-04(06)	cross-organization management of identifiers is coordinated with ***<IA-04(06)_ODP external organizations>***.

IA-04(06)	IDENTIFIER MANAGEMENT | CROSS-ORGANIZATION MANAGEMENT	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-04(06)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; system security plan; other relevant documents or records].
	IA-04(06)-Interview	[SELECT FROM: Organizational personnel with identifier management responsibilities; organizational personnel with information security responsibilities].
	IA-04(06)-Test	[SELECT FROM: Mechanisms supporting and/or implementing identifier management].

IA-04(07)	IDENTIFIER MANAGEMENT | IN-PERSON REGISTRATION
	[WITHDRAWN: Incorporated into IA-12(04).]

IA-04(08)	IDENTIFIER MANAGEMENT | PAIRWISE PSEUDONYMOUS IDENTIFIERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-04(08)	pairwise pseudonymous identifiers are generated.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-04(08)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing identifier management; procedures addressing account management; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	IA-04(08)-Interview	[SELECT FROM: Organizational personnel with identifier management responsibilities; organizational personnel with information security responsibilities].
	IA-04(08)-Test	[SELECT FROM: Mechanisms supporting and/or implementing identifier management].

IA-04(09)	IDENTIFIER MANAGEMENT | ATTRIBUTE MAINTENANCE AND PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-04(09)_ODP	***protected central storage used to maintain the attributes for each uniquely identified individual, device, or service is defined;***
	IA-04(09)	the attributes for each uniquely identified individual, device, or service are maintained in ***<IA-04(09)_ODP protected central storage>***.

IA-04(09)	IDENTIFIER MANAGEMENT | ATTRIBUTE MAINTENANCE AND PROTECTION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-04(09)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing identifier management; procedures addressing account management; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	IA-04(09)-Interview	[SELECT FROM: Organizational personnel with identifier management responsibilities; organizational personnel with information security responsibilities].
	IA-04(09)-Test	[SELECT FROM: Mechanisms supporting and/or implementing identifier management].

IA-05	AUTHENTICATOR MANAGEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-05_ODP[01]	***a time period for changing or refreshing authenticators by authenticator type is defined;***
	IA-05_ODP[02]	***events that trigger the change or refreshment of authenticators are defined;***
	IA-05a.	system authenticators are managed through the verification of the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution;
	IA-05b.	system authenticators are managed through the establishment of initial authenticator content for any authenticators issued by the organization;
	IA-05c.	system authenticators are managed to ensure that authenticators have sufficient strength of mechanism for their intended use;
	IA-05d.	system authenticators are managed through the establishment and implementation of administrative procedures for initial authenticator distribution; lost, compromised, or damaged authenticators; and the revocation of authenticators;
	IA-05e.	system authenticators are managed through the change of default authenticators prior to first use;
	IA-05f.	system authenticators are managed through the change or refreshment of authenticators ***<IA-05_ODP[01] time period by authenticator type>*** or when ***<IA-05_ODP[02] events>*** occur;
	IA-05g.	system authenticators are managed through the protection of authenticator content from unauthorized disclosure and modification;
	IA-05h.[01]	system authenticators are managed through the requirement for individuals to take specific controls to protect authenticators;
	IA-05h.[02]	system authenticators are managed through the requirement for devices to implement specific controls to protect authenticators;
	IA-05i.	system authenticators are managed through the change of authenticators for group or role accounts when membership to those accounts changes.

IA-05	AUTHENTICATOR MANAGEMENT	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-05-Examine	[SELECT FROM: Identification and authentication policy; system security plan; addressing authenticator management; system design documentation; system configuration settings and associated documentation; list of system authenticator types; change control records associated with managing system authenticators; system audit records; other relevant documents or records].
	IA-05-Interview	[SELECT FROM: Organizational personnel with authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	IA-05-Test	[SELECT FROM: Mechanisms supporting and/or implementing authenticator management capability].

IA-05(01)	AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-05(01)_ODP[01]	***the frequency at which to update the list of commonly used, expected, or compromised passwords is defined;***
	IA-05(01)_ODP[02]	***authenticator composition and complexity rules are defined;***
	IA-05(01)(a)	for password-based authentication, a list of commonly used, expected, or compromised passwords is maintained and updated ***<IA-05(01)_ODP[01] frequency>*** and when organizational passwords are suspected to have been compromised directly or indirectly;
	IA-05(01)(b)	for password-based authentication when passwords are created or updated by users, the passwords are verified not to be found on the list of commonly used, expected, or compromised passwords in IA-05(01)(a);
	IA-05(01)(c)	for password-based authentication, passwords are only transmitted over cryptographically protected channels;
	IA-05(01)(d)	for password-based authentication, passwords are stored using an approved salted key derivation function, preferably using a keyed hash;
	IA-05(01)(e)	for password-based authentication, immediate selection of a new password is required upon account recovery;
	IA-05(01)(f)	for password-based authentication, user selection of long passwords and passphrases is allowed, including spaces and all printable characters;
	IA-05(01)(g)	for password-based authentication, automated tools are employed to assist the user in selecting strong password authenticators;
	IA-05(01)(h)	for password-based authentication, ***<IA-05(01)_ODP[02] composition and complexity rules>*** are enforced.

IA-05(01)	AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-05(01)-Examine	[SELECT FROM: Identification and authentication policy; password policy; procedures addressing authenticator management; system security plan; system design documentation; system configuration settings and associated documentation; password configurations and associated documentation; other relevant documents or records].
	IA-05(01)-Interview	[SELECT FROM: Organizational personnel with authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-05(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing password-based authenticator management capability].

IA-05(02)	AUTHENTICATOR MANAGEMENT | PUBLIC KEY-BASED AUTHENTICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-05(02)(a)(01)	authorized access to the corresponding private key is enforced for public key-based authentication;
	IA-05(02)(a)(02)	the authenticated identity is mapped to the account of the individual or group for public key-based authentication;
	IA-05(02)(b)(01)	when public key infrastructure (PKI) is used, certificates are validated by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information;
	IA-05(02)(b)(02)	when public key infrastructure (PKI) is used, a local cache of revocation data is implemented to support path discovery and validation.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-05(02)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing authenticator management; system security plan; system design documentation; system configuration settings and associated documentation; PKI certification validation records; PKI certification revocation lists; other relevant documents or records].
	IA-05(02)-Interview	[SELECT FROM: Organizational personnel with PKI-based, authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-05(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing PKI-based, authenticator management capability].

IA-05(03)	AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED EXTERNAL PARTY REGISTRATION
	[WITHDRAWN: Incorporated into IA-12(04).]

IA-05(04)	AUTHENTICATOR MANAGEMENT | AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION
	[WITHDRAWN: Incorporated into IA-05(01).]

IA-05(05)	AUTHENTICATOR MANAGEMENT | CHANGE AUTHENTICATORS PRIOR TO DELIVERY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-05(05)	developers and installers of system components are required to provide unique authenticators or change default authenticators prior to delivery and installation.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-05(05)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; system and services acquisition policy; procedures addressing authenticator management; procedures addressing the integration of security requirements into the acquisition process; acquisition documentation; acquisition contracts for system procurements or services; other relevant documents or records].
	IA-05(05)-Interview	[SELECT FROM: Organizational personnel with authenticator management responsibilities; organizational personnel with information security, acquisition, and contracting responsibilities; system developers].
	IA-05(05)-Test	[SELECT FROM: Mechanisms supporting and/or implementing authenticator management capability].

IA-05(06)	AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-05(06)	authenticators are protected commensurate with the security category of the information to which use of the authenticator permits access.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-05(06)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing authenticator management; security categorization documentation for the system; security assessments of authenticator protections; risk assessment results; system security plan; other relevant documents or records].
	IA-05(06)-Interview	[SELECT FROM: Organizational personnel with authenticator management responsibilities; organizational personnel implementing and/or maintaining authenticator protections; organizational personnel with information security responsibilities; system/network administrators].
	IA-05(06)-Test	[SELECT FROM: Mechanisms supporting and/or implementing authenticator management capability; mechanisms protecting authenticators].

IA-05(07)	AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-05(07)	unencrypted static authenticators are not embedded in applications or other forms of static storage.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-05(07)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing authenticator management; system design documentation; system configuration settings and associated documentation; logical access scripts; application code reviews for detecting unencrypted static authenticators; other relevant documents or records].
	IA-05(07)-Interview	[SELECT FROM: Organizational personnel with authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-05(07)-Test	[SELECT FROM: Mechanisms supporting and/or implementing authenticator management capability; mechanisms implementing authentication in applications].

IA-05(08)	AUTHENTICATOR MANAGEMENT | MULTIPLE SYSTEM ACCOUNTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-05(08)_ODP	***security controls implemented to manage the risk of compromise due to individuals having accounts on multiple systems are defined;***
	IA-05(08)	***<IA-05(08)_ODP security controls>*** are implemented to manage the risk of compromise due to individuals having accounts on multiple systems.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-05(08)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing authenticator management; system security plan; list of individuals having accounts on multiple systems; list of security safeguards intended to manage risk of compromise due to individuals having accounts on multiple systems; other relevant documents or records].
	IA-05(08)-Interview	[SELECT FROM: Organizational personnel with authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	IA-05(08)-Test	[SELECT FROM: Mechanisms supporting and/or implementing safeguards for authenticator management].

IA-05(09)	AUTHENTICATOR MANAGEMENT | FEDERATED CREDENTIAL MANAGEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-05(09)_ODP	***external organizations to be used for federating credentials are defined;***

IA-05(09)	AUTHENTICATOR MANAGEMENT | FEDERATED CREDENTIAL MANAGEMENT	
	IA-05(09)	***<IA-05(09)_ODP external organizations>*** are used to federate credentials.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-05(09)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing authenticator management; procedures addressing account management; system security plan; security agreements; other relevant documents or records].
	IA-05(09)-Interview	[SELECT FROM: Organizational personnel with authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	IA-05(09)-Test	[SELECT FROM: Mechanisms supporting and/or implementing safeguards for authenticator management].

IA-05(10)	AUTHENTICATOR MANAGEMENT | DYNAMIC CREDENTIAL BINDING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-05(10)_ODP	***rules for dynamically binding identities and authenticators are defined;***
	IA-05(10)	identities and authenticators are dynamically bound using ***<IA-05(10)_ODP binding rules>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-05(10)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing identifier management; system security plan; system design documentation; automated mechanisms providing dynamic binding of identifiers and authenticators; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	IA-05(10)-Interview	[SELECT FROM: Organizational personnel with identifier management responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	IA-05(10)-Test	[SELECT FROM: Automated mechanisms implementing identifier management capability; automated mechanisms implementing dynamic binding of identities and authenticators].

IA-05(11)	AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION
	[WITHDRAWN: Incorporated into IA-02(01), IA-02(02).]

IA-05(12)	AUTHENTICATOR MANAGEMENT | BIOMETRIC AUTHENTICATION PERFORMANCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-05(12)_ODP	***biometric quality requirements for biometric-based authentication are defined;***

IA-05(12)	AUTHENTICATOR MANAGEMENT | BIOMETRIC AUTHENTICATION PERFORMANCE	
	IA-05(12)	mechanisms that satisfy ***<IA-05(12)_ODP biometric quality requirements>*** are employed for biometric-based authentication.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-05(12)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing authenticator management; system security plan; system design documentation; mechanisms employing biometric-based authentication for the system; list of biometric quality requirements; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	IA-05(12)-Interview	[SELECT FROM: Organizational personnel with authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-05(12)-Test	[SELECT FROM: Mechanisms supporting and/or implementing biometric-based authenticator management capability].

IA-05(13)	AUTHENTICATOR MANAGEMENT | EXPIRATION OF CACHED AUTHENTICATORS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-05(13)_ODP	***the time period after which the use of cached authenticators is prohibited is defined;***
	IA-05(13)	the use of cached authenticators is prohibited after ***<IA-05(13)_ODP time period>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-05(13)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing authenticator management; system security plan; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	IA-05(13)-Interview	[SELECT FROM: Organizational personnel with authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-05(13)-Test	[SELECT FROM: Mechanisms supporting and/or implementing authenticator management capability].

IA-05(14)	AUTHENTICATOR MANAGEMENT | MANAGING CONTENT OF PKI TRUST STORES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-05(14)	an organization-wide methodology for managing the content of PKI trust stores is employed across all platforms, including networks, operating systems, browsers, and applications for PKI-based authentication.

IA-05(14)	AUTHENTICATOR MANAGEMENT | MANAGING CONTENT OF PKI TRUST STORES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-05(14)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing authenticator management; system security plan; organizational methodology for managing content of PKI trust stores across installed all platforms; system design documentation; system configuration settings and associated documentation; enterprise security architecture documentation; enterprise architecture documentation; other relevant documents or records].
	IA-05(14)-Interview	[SELECT FROM: Organizational personnel with authenticator management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-05(14)-Test	[SELECT FROM: Mechanisms supporting and/or implementing PKI-based authenticator management capability; mechanisms supporting and/or implementing the PKI trust store capability].

IA-05(15)	AUTHENTICATOR MANAGEMENT | GSA-APPROVED PRODUCTS AND SERVICES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-05(15)	only General Services Administration-approved products and services are used for identity, credential, and access management.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-05(15)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing identifier management; system security plan; system design documentation; mechanisms providing dynamic binding of identifiers and authenticators; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	IA-05(15)-Interview	[SELECT FROM: Organizational personnel with identification and authentication management responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	IA-05(15)-Test	[SELECT FROM: Mechanisms supporting and/or implementing account management capability; mechanisms supporting and/or implementing identification and authentication management capabilities for the system].

IA-05(16)	AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED EXTERNAL PARTY AUTHENTICATOR ISSUANCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-05(16)_ODP[01]	***types of and/or specific authenticators to be issued are defined;***
	IA-05(16)_ODP[02]	***one of the following PARAMETER VALUES is selected: {in person; by a trusted external party};***
	IA-05(16)_ODP[03]	***the registration authority that issues authenticators is defined;***

IA-05(16)	AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED EXTERNAL PARTY AUTHENTICATOR ISSUANCE	
	IA-05(16)_ODP[04]	***the personnel or roles who authorize the issuance of authenticators are defined;***
	IA-05(16)	the issuance of ***<IA-05(16)_ODP[01] types of and/or specific authenticators>*** is required to be conducted ***<IA-05(16)_ODP[02] SELECTED PARAMETER VALUE>*** before ***<IA-05(16)_ODP[03] registration authority>*** with authorization by ***<IA-05(16)_ODP[04] personnel or roles>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-05(16)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing identifier management; system security plan; system design documentation; mechanisms providing dynamic binding of identifiers and authenticators; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	IA-05(16)-Interview	[SELECT FROM: Organizational personnel with identification and authentication management responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	IA-05(16)-Test	[SELECT FROM: Mechanisms supporting and/or implementing account management capability; mechanisms supporting and/or implementing identification and authentication management capabilities for the system].

IA-05(17)	AUTHENTICATOR MANAGEMENT | PRESENTATION ATTACK DETECTION FOR BIOMETRIC AUTHENTICATORS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-05(17)	presentation attack detection mechanisms are employed for biometric-based authentication.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-05(17)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing identifier management; system security plan; system design documentation; mechanisms providing dynamic binding of identifiers and authenticators; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	IA-05(17)-Interview	[SELECT FROM: Organizational personnel with identification and authentication management responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	IA-05(17)-Test	[SELECT FROM: Mechanisms supporting and/or implementing account management capability; mechanisms supporting and/or implementing identification and authentication management capabilities for the system].

IA-05(18)	AUTHENTICATOR MANAGEMENT | PASSWORD MANAGERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-05(18)_ODP[01]	***password managers employed for generating and managing passwords are defined;***
	IA-05(18)_ODP[02]	***controls for protecting passwords are defined;***
	IA-05(18)(a)	***<IA-05(18)_ODP[01] password managers>*** are employed to generate and manage passwords;
	IA-05(18)(b)	the passwords are protected using ***<IA-05(18)_ODP[02] controls>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-05(18)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing identifier management; system security plan; system design documentation; mechanisms providing dynamic binding of identifiers and authenticators; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	IA-05(18)-Interview	[SELECT FROM: Organizational personnel with identification and authentication management responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	IA-05(18)-Test	[SELECT FROM: Mechanisms supporting and/or implementing account management capability; mechanisms supporting and/or implementing identification and authentication management capabilities for the system].

IA-06	AUTHENTICATION FEEDBACK	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-06	the feedback of authentication information is obscured during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-06-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing authenticator feedback; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	IA-06-Interview	[SELECT FROM: Organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-06-Test	[SELECT FROM: Mechanisms supporting and/or implementing the obscuring of feedback of authentication information during authentication].

IA-07	CRYPTOGRAPHIC MODULE AUTHENTICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-07	mechanisms for authentication to a cryptographic module are implemented that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-07-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing cryptographic module authentication; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	IA-07-Interview	[SELECT FROM: Organizational personnel with responsibility for cryptographic module authentication; organizational personnel with information security responsibilities; system/network administrators; system developers].
	IA-07-Test	[SELECT FROM: Mechanisms supporting and/or implementing cryptographic module authentication].

IA-08	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-08	non-organizational users or processes acting on behalf of non-organizational users are uniquely identified and authenticated.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-08-Examine	[SELECT FROM: Identification and authentication policy; system security plan; privacy plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; list of system accounts; other relevant documents or records].
	IA-08-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; organizational personnel with account management responsibilities].
	IA-08-Test	[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities].

IA-08(01)	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-08(01)[01]	Personal Identity Verification-compliant credentials from other federal agencies are accepted;

IA-08(01)	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES	
	IA-08(01)[02]	Personal Identity Verification-compliant credentials from other federal agencies are electronically verified.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-08(01)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; PIV verification records; evidence of PIV credentials; PIV credential authorizations; other relevant documents or records].
	IA-08(01)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/ network administrators; system developers; organizational personnel with account management responsibilities].
	IA-08(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities; mechanisms that accept and verify PIV credentials].

IA-08(02)	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF EXTERNAL AUTHENTICATORS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-08(02)(a)	only external authenticators that are NIST-compliant are accepted;
	IA-08(02)(b)[01]	a list of accepted external authenticators is documented;
	IA-08(02)(b)[02]	a list of accepted external authenticators is maintained.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-08(02)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; list of third-party credentialing products, components, or services procured and implemented by organization; third-party credential verification records; evidence of third-party credentials; third-party credential authorizations; other relevant documents or records].
	IA-08(02)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/ network administrators; system developers; organizational personnel with account management responsibilities].
	IA-08(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities; mechanisms that accept external credentials].

IA-08(03)	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-APPROVED PRODUCTS
	[WITHDRAWN: Incorporated into IA-08(02).]

IA-08(04)	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF DEFINED PROFILES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-08(04)_ODP	***identity management profiles are defined;***
	IA-08(04)	there is conformance with ***<IA-08(04)_ODP identity management profiles>*** for identity management.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-08(04)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	IA-08(04)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/ network administrators; system developers; organizational personnel with account management responsibilities].
	IA-08(04)-Test	[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities; mechanisms supporting and/or implementing conformance with profiles].

IA-08(05)	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV-I CREDENTIALS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-08(05)_ODP	***a policy for using federated or PKI credentials is defined;***
	IA-08(05)[01]	federated or PKI credentials that meet ***<IA-08(05)_ODP policy>*** are accepted;
	IA-08(05)[02]	federated or PKI credentials that meet ***<IA-08(05)_ODP policy>*** are verified.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-08(05)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; PIV-I verification records; evidence of PIV-I credentials; PIV-I credential authorizations; other relevant documents or records].
	IA-08(05)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/ network administrators; system developers; organizational personnel with account management responsibilities].

IA-08(05)	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV-I CREDENTIALS	
	IA-08(05)-Test	[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities; mechanisms that accept and verify PIV-I credentials].

IA-08(06)	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | DISASSOCIABILITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-08(06)_ODP	***disassociability measures are defined;***
	IA-08(06)	***<IA-08(06)_ODP measures>*** to disassociate user attributes or identifier assertion relationships among individuals, credential service providers, and relying parties are implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-08(06)-Examine	[SELECT FROM: Identification and authentication policy; system security plan; privacy plan; procedures addressing user identification and authentication; system design documentation; system configuration settings and associated documentation; system audit records; other relevant documents or records].
	IA-08(06)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers; organizational personnel with account management responsibilities].
	IA-08(06)-Test	[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities].

IA-09	SERVICE IDENTIFICATION AND AUTHENTICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-09_ODP	***system services and applications to be uniquely identified and authenticated are defined;***
	IA-09	***<IA-09_ODP system services and applications>*** are uniquely identified and authenticated before establishing communications with devices, users, or other services or applications.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-09-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing service identification and authentication; system security plan; system design documentation; security safeguards used to identify and authenticate system services; system configuration settings and associated documentation; system audit records; other relevant documents or records].

IA-09	SERVICE IDENTIFICATION AND AUTHENTICATION	
	IA-09-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; organizational personnel with identification and authentication responsibilities].
	IA-09-Test	[SELECT FROM: Security safeguards implementing service identification and authentication capabilities].

IA-09(01)	SERVICE IDENTIFICATION AND AUTHENTICATION | INFORMATION EXCHANGE	
	[WITHDRAWN: Incorporated into IA-09.]	

IA-09(02)	SERVICE IDENTIFICATION AND AUTHENTICATION | TRANSMISSION OF DECISIONS	
	[WITHDRAWN: Incorporated into IA-09.]	

IA-10	ADAPTIVE AUTHENTICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-10_ODP[01]	***supplemental authentication techniques or mechanisms to be employed when accessing the system under specific circumstances or situations are defined;***
	IA-10_ODP[02]	***circumstances or situations that require individuals accessing the system to employ supplemental authentication techniques or mechanisms are defined;***
	IA-10	individuals accessing the system are required to employ ***<IA-10_ODP[01] supplemental authentication techniques or mechanisms>*** under specific ***<IA-10_ODP[02] circumstances or situations>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-10-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing adaptive/supplemental identification and authentication techniques or mechanisms; system security plan; system design documentation; system configuration settings and associated documentation; supplemental identification and authentication techniques or mechanisms; system audit records; other relevant documents or records].
	IA-10-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; organizational personnel with identification and authentication responsibilities].
	IA-10-Test	[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities].

IA-11	RE-AUTHENTICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-11_ODP	***circumstances or situations requiring re-authentication are defined;***
	IA-11	users are required to re-authenticate when ***<IA-11_ODP circumstances or situations>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-11-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing user and device re-authentication; system security plan; system design documentation; system configuration settings and associated documentation; list of circumstances or situations requiring re-authentication; system audit records; other relevant documents or records].
	IA-11-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; organizational personnel with identification and authentication responsibilities].
	IA-11-Test	[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities].

IA-12	IDENTITY PROOFING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-12a.	users who require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines are identity proofed;
	IA-12b.	user identities are resolved to a unique individual;
	IA-12c.[01]	identity evidence is collected;
	IA-12c.[02]	identity evidence is validated;
	IA-12c.[03]	identity evidence is verified.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-12-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing identity proofing; system security plan; privacy plan; other relevant documents or records].
	IA-12-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security and privacy responsibilities; legal counsel; system/network administrators; system developers; organizational personnel with identification and authentication responsibilities].
	IA-12-Test	[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities].

IA-12(01)	IDENTITY PROOFING | SUPERVISOR AUTHORIZATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-12(01)	the registration process to receive an account for logical access includes supervisor or sponsor authorization.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-12(01)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing identity proofing; system security plan; other relevant documents or records].
	IA-12(01)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; organizational personnel with identification and authentication responsibilities].
	IA-12(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities].

IA-12(02)	IDENTITY PROOFING | IDENTITY EVIDENCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-12(02)	evidence of individual identification is presented to the registration authority.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-12(02)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing identity proofing; system security plan; other relevant documents or records].
	IA-12(02)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; organizational personnel with identification and authentication responsibilities].
	IA-12(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities].

IA-12(03)	IDENTITY PROOFING | IDENTITY EVIDENCE VALIDATION AND VERIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-12(03)_ODP	***methods of validation and verification of identity evidence are defined;***
	IA-12(03)	the presented identity evidence is validated and verified through ***<IA-12(03)_ODP methods of validation and verification>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-12(03)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing identity proofing; system security plan; other relevant documents or records].

IA-12(03)	IDENTITY PROOFING | IDENTITY EVIDENCE VALIDATION AND VERIFICATION	
	IA-12(03)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; organizational personnel with identification and authentication responsibilities].
	IA-12(03)-Test	[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities].

IA-12(04)	IDENTITY PROOFING | IN-PERSON VALIDATION AND VERIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-12(04)	the validation and verification of identity evidence is conducted in person before a designated registration authority.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-12(04)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing identity proofing; system security plan; other relevant documents or records].
	IA-12(04)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; organizational personnel with identification and authentication responsibilities].
	IA-12(04)-Test	[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities].

IA-12(05)	IDENTITY PROOFING | ADDRESS CONFIRMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-12(05)_ODP	***one of the following PARAMETER VALUES is selected: {registration code; notice of proofing};***
	IA-12(05)	a ***<IA-12(05)_ODP SELECTED PARAMETER VALUE>*** is delivered through an out-of-band channel to verify the user's address (physical or digital) of record.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-12(05)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing identity proofing; system security plan; other relevant documents or records].
	IA-12(05)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; organizational personnel with identification and authentication responsibilities].
	IA-12(05)-Test	[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities].

IA-12(06)	IDENTITY PROOFING | ACCEPT EXTERNALLY-PROOFED IDENTITIES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IA-12(06)_ODP	***an identity assurance level for accepting externally proofed identities is defined;***
	IA-12(06)	externally proofed identities are accepted ***<IA-12(06)_ODP identity assurance level>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IA-12(06)-Examine	[SELECT FROM: Identification and authentication policy; procedures addressing identity proofing; system security plan; other relevant documents or records].
	IA-12(06)-Interview	[SELECT FROM: Organizational personnel with system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers; organizational personnel with identification and authentication responsibilities].
	IA-12(06)-Test	[SELECT FROM: Mechanisms supporting and/or implementing identification and authentication capabilities].

4.8 INCIDENT RESPONSE

IR-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-01_ODP[01]	***personnel or roles to whom the incident response policy is to be disseminated is/are defined;***
	IR-01_ODP[02]	***personnel or roles to whom the incident response procedures are to be disseminated is/are defined;***
	IR-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	IR-01_ODP[04]	***an official to manage the incident response policy and procedures is defined;***
	IR-01_ODP[05]	***the frequency at which the current incident response policy is reviewed and updated is defined;***
	IR-01_ODP[06]	***events that would require the current incident response policy to be reviewed and updated are defined;***
	IR-01_ODP[07]	***the frequency at which the current incident response procedures are reviewed and updated is defined;***
	IR-01_ODP[08]	***events that would require the incident response procedures to be reviewed and updated are defined;***
	IR-01a.[01]	an incident response policy is developed and documented;
	IR-01a.[02]	the incident response policy is disseminated to ***<IR-01_ODP[01] personnel or roles>***;
	IR-01a.[03]	incident response procedures to facilitate the implementation of the incident response policy and associated incident response controls are developed and documented;
	IR-01a.[04]	the incident response procedures are disseminated to ***<IR-01_ODP[02] personnel or roles>***;
	IR-01a.01(a)[01]	the ***<IR-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** incident response policy addresses purpose;
	IR-01a.01(a)[02]	the ***<IR-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** incident response policy addresses scope;
	IR-01a.01(a)[03]	the ***<IR-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** incident response policy addresses roles;
	IR-01a.01(a)[04]	the ***<IR-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** incident response policy addresses responsibilities;
	IR-01a.01(a)[05]	the ***<IR-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** incident response policy addresses management commitment;
	IR-01a.01(a)[06]	the ***<IR-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** incident response policy addresses coordination among organizational entities;
	IR-01a.01(a)[07]	the ***<IR-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** incident response policy addresses compliance;

IR-01	POLICY AND PROCEDURES	
	IR-01a.01(b)	the ***<IR-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** incident response policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines;
	IR-01b.	the ***<IR-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the incident response policy and procedures;
	IR-01c.01[01]	the current incident response policy is reviewed and updated ***<IR-01_ODP[05] frequency>***;
	IR-01c.01[02]	the current incident response policy is reviewed and updated following ***<IR-01_ODP[06] events>***;
	IR-01c.02[01]	the current incident response procedures are reviewed and updated ***<IR-01_ODP[07] frequency>***;
	IR-01c.02[02]	the current incident response procedures are reviewed and updated following ***<IR-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-01-Examine	[SELECT FROM: Incident response policy and procedures; system security plan; privacy plan; other relevant documents or records].
	IR-01-Interview	[SELECT FROM: Organizational personnel with incident response responsibilities; organizational personnel with information security and privacy responsibilities].

IR-02	INCIDENT RESPONSE TRAINING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-02_ODP[01]	***a time period within which incident response training is to be provided to system users assuming an incident response role or responsibility is defined;***
	IR-02_ODP[02]	***frequency at which to provide incident response training to users is defined;***
	IR-02_ODP[03]	***frequency at which to review and update incident response training content is defined;***
	IR-02_ODP[04]	***events that initiate a review of the incident response training content are defined;***
	IR-02a.01	incident response training is provided to system users consistent with assigned roles and responsibilities within ***<IR-02_ODP[01] time period>*** of assuming an incident response role or responsibility or acquiring system access;
	IR-02a.02	incident response training is provided to system users consistent with assigned roles and responsibilities when required by system changes;
	IR-02a.03	incident response training is provided to system users consistent with assigned roles and responsibilities ***<IR-02_ODP[02] frequency>*** thereafter;
	IR-02b.[01]	incident response training content is reviewed and updated ***<IR-02_ODP[03] frequency>***;
	IR-02b.[02]	incident response training content is reviewed and updated following ***<IR-02_ODP[04] events>***.

IR-02	INCIDENT RESPONSE TRAINING	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-02-Examine	[SELECT FROM: Incident response policy; procedures addressing incident response training; incident response training curriculum; incident response training materials; privacy plan; incident response plan; incident response training records; system security plan; privacy plan; other relevant documents or records].
	IR-02-Interview	[SELECT FROM: Organizational personnel with incident response training and operational responsibilities; organizational personnel with information security and privacy responsibilities].

IR-02(01)	INCIDENT RESPONSE TRAINING | SIMULATED EVENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-02(01)	simulated events are incorporated into incident response training to facilitate the required response by personnel in crisis situations.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-02(01)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident response training; incident response training curriculum; incident response training materials; incident response plan; system security plan; privacy plan; other relevant documents or records].
	IR-02(01)-Interview	[SELECT FROM: Organizational personnel with incident response training and operational responsibilities; organizational personnel with information security and privacy responsibilities].
	IR-02(01)-Test	[SELECT FROM: Mechanisms that support and/or implement simulated events for incident response training].

IR-02(02)	INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-02(02)_ODP	***automated mechanisms used in an incident response training environment are defined;***
	IR-02(02)	an incident response training environment is provided using ***<IR-02(02)_ODP automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-02(02)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident response training; incident response training curriculum; incident response training materials; automated mechanisms supporting incident response training; incident response plan; system security plan; privacy plan; other relevant documents or records].

IR-02(02)	INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS	
	IR-02(02)-Interview	[SELECT FROM: Organizational personnel with incident response training and operational responsibilities; organizational personnel with information security and privacy responsibilities].
	IR-02(02)-Test	[SELECT FROM: Automated mechanisms that provide a thorough and realistic incident response training environment].

IR-02(03)	INCIDENT RESPONSE TRAINING | BREACH	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-02(03)[01]	incident response training on how to identify and respond to a breach is provided;
	IR-02(03)[02]	incident response training on the organization's process for reporting a breach is provided.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-02(03)-Examine	[SELECT FROM: Incident response policy; contingency planning policy; procedures addressing incident response testing; procedures addressing contingency plan testing; incident response testing material; incident response test results; incident response test plan; incident response plan; contingency plan; system security plan; privacy plan; other relevant documents or records].
	IR-02(03)-Interview	[SELECT FROM: Organizational personnel with incident response training responsibilities; organizational personnel with information security and privacy responsibilities].

IR-03	INCIDENT RESPONSE TESTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-03_ODP[01]	***frequency at which to test the effectiveness of the incident response capability for the system is defined;***
	IR-03_ODP[02]	***tests used to test the effectiveness of the incident response capability for the system are defined;***
	IR-03	the effectiveness of the incident response capability for the system is tested ***<IR-03_ODP[01] frequency>*** using ***<IR-03_ODP[02] tests>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-03-Examine	[SELECT FROM: Incident response policy; contingency planning policy; procedures addressing incident response testing; procedures addressing contingency plan testing; incident response testing material; incident response test results; incident response test plan; incident response plan; contingency plan; system security plan; privacy plan; other relevant documents or records].
	IR-03-Interview	[SELECT FROM: Organizational personnel with incident response testing responsibilities; organizational personnel with information security and privacy responsibilities].

IR-03(01)	INCIDENT RESPONSE TESTING | AUTOMATED TESTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-03(01)_ODP	***automated mechanisms used to test the incident response capability are defined;***
	IR-03(01)	the incident response capability is tested using ***<IR-03(01)_ODP automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-03(01)-Examine	[SELECT FROM: Incident response policy; contingency planning policy; procedures addressing incident response testing; procedures addressing contingency plan testing; incident response testing documentation; incident response test results; incident response test plan; incident response plan; contingency plan; system security plan; automated mechanisms supporting incident response tests; other relevant documents or records].
	IR-03(01)-Interview	[SELECT FROM: Organizational personnel with incident response testing responsibilities; organizational personnel with information security responsibilities].
	IR-03(01)-Test	[SELECT FROM: Automated mechanisms that more thoroughly and effectively test the incident response capability].

IR-03(02)	INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-03(02)	incident response testing is coordinated with organizational elements responsible for related plans.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-03(02)-Examine	[SELECT FROM: Incident response policy; contingency planning policy; procedures addressing incident response testing; incident response testing documentation; incident response plan; business continuity plans; contingency plans; disaster recovery plans; continuity of operations plans; crisis communications plans; critical infrastructure plans; occupant emergency plans; system security plan; privacy plan; other relevant documents or records].
	IR-03(02)-Interview	[SELECT FROM: Organizational personnel with incident response testing responsibilities; organizational personnel with responsibilities for testing organizational plans related to incident response testing; organizational personnel with information security and privacy responsibilities].

IR-03(03)	INCIDENT RESPONSE TESTING | CONTINUOUS IMPROVEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-03(03)(a)[01]	qualitative data from testing are used to determine the effectiveness of incident response processes;

IR-03(03)	INCIDENT RESPONSE TESTING | CONTINUOUS IMPROVEMENT	
	IR-03(03)(a)[02]	quantitative data from testing are used to determine the effectiveness of incident response processes;
	IR-03(03)(b)[01]	qualitative data from testing are used to continuously improve incident response processes;
	IR-03(03)(b)[02]	quantitative data from testing are used to continuously improve incident response processes;
	IR-03(03)(c)[01]	qualitative data from testing are used to provide incident response measures and metrics that are accurate;
	IR-03(03)(c)[02]	quantitative data from testing are used to provide incident response measures and metrics that are accurate;
	IR-03(03)(c)[03]	qualitative data from testing are used to provide incident response measures and metrics that are consistent;
	IR-03(03)(c)[04]	quantitative data from testing are used to provide incident response measures and metrics that are consistent;
	IR-03(03)(c)[05]	qualitative data from testing are used to provide incident response measures and metrics in a reproducible format;
	IR-03(03)(c)[06]	quantitative data from testing are used to provide incident response measures and metrics in a reproducible format.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-03(03)-Examine	[SELECT FROM: Incident response policy; contingency planning policy; procedures addressing incident response testing; incident response testing documentation; incident response plan; business continuity plans; contingency plans; disaster recovery plans; continuity of operations plans; crisis communications plans; critical infrastructure plans; occupant emergency plans; system security plan; privacy plan; other relevant documents or records].
	IR-03(03)-Interview	[SELECT FROM: Organizational personnel with incident response testing responsibilities; organizational personnel with responsibilities for testing organizational plans related to incident response testing; organizational personnel with information security and privacy responsibilities].

IR-04	INCIDENT HANDLING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-04a.[01]	an incident handling capability for incidents is implemented that is consistent with the incident response plan;
	IR-04a.[02]	the incident handling capability for incidents includes preparation;
	IR-04a.[03]	the incident handling capability for incidents includes detection and analysis;
	IR-04a.[04]	the incident handling capability for incidents includes containment;
	IR-04a.[05]	the incident handling capability for incidents includes eradication;
	IR-04a.[06]	the incident handling capability for incidents includes recovery;

IR-04	INCIDENT HANDLING	
	IR-04b.	incident handling activities are coordinated with contingency planning activities;
	IR-04c.[01]	lessons learned from ongoing incident handling activities are incorporated into incident response procedures, training, and testing;
	IR-04c.[02]	the changes resulting from the incorporated lessons learned are implemented accordingly;
	IR-04d.[01]	the rigor of incident handling activities is comparable and predictable across the organization;
	IR-04d.[02]	the intensity of incident handling activities is comparable and predictable across the organization;
	IR-04d.[03]	the scope of incident handling activities is comparable and predictable across the organization;
	IR-04d.[04]	the results of incident handling activities are comparable and predictable across the organization.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-04-Examine	[SELECT FROM: Incident response policy; contingency planning policy; procedures addressing incident handling; incident response plan; contingency plan; system security plan; privacy plan; other relevant documents or records].
	IR-04-Interview	[SELECT FROM: Organizational personnel with incident handling responsibilities; organizational personnel with contingency planning responsibilities; organizational personnel with information security and privacy responsibilities].
	IR-04-Test	[SELECT FROM: Incident handling capability for the organization].

IR-04(01)	INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-04(01)_ODP	***automated mechanisms used to support the incident handling process are defined;***
	IR-04(01)	the incident handling process is supported using ***<IR-04(01)_ODP automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-04(01)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; system design documentation; system configuration settings and associated documentation; system audit records; incident response plan; system security plan; other relevant documents or records].
	IR-04(01)-Interview	[SELECT FROM: Organizational personnel with incident handling responsibilities; organizational personnel with information security responsibilities].
	IR-04(01)-Test	[SELECT FROM: Automated mechanisms that support and/or implement the incident handling process].

IR-04(02)	INCIDENT HANDLING | DYNAMIC RECONFIGURATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-04(02)_ODP[01]	***types of dynamic reconfiguration for system components are defined;***
	IR-04(02)_ODP[02]	***system components that require dynamic reconfiguration are defined;***
	IR-04(02)	***<IR-04(02)_ODP[01] types of dynamic reconfiguration>*** for ***<IR-04(02)_ODP[02] system components>*** are included as part of the incident response capability.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-04(02)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident handling; mechanisms supporting incident handling; list of system components to be dynamically reconfigured as part of incident response capability; system design documentation; system configuration settings and associated documentation; system audit records; incident response plan; system security plan; other relevant documents or records].
	IR-04(02)-Interview	[SELECT FROM: Organizational personnel with incident handling responsibilities; organizational personnel with information security responsibilities].
	IR-04(02)-Test	[SELECT FROM: Mechanisms that support and/or implement the dynamic reconfiguration of components as part of incident response].

IR-04(03)	INCIDENT HANDLING | CONTINUITY OF OPERATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-04(03)_ODP[01]	***classes of incidents requiring an organization-defined action (defined in IR-04(03)_ODP[02]) to be taken are defined;***
	IR-04(03)_ODP[02]	***actions to be taken in response to organization-defined classes of incidents are defined;***
	IR-04(03)[01]	***<IR-04(03)_ODP[01] classes of incidents>*** are identified;
	IR-04(03)[02]	***<IR-04(03)_ODP[02] actions>*** are taken in response to those incidents (defined in IR-04(03)_ODP[01]) to ensure the continuation of organizational mission and business functions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-04(03)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident handling; incident response plan; privacy plan; list of classes of incidents; list of appropriate incident response actions; system security plan; other relevant documents or records].
	IR-04(03)-Interview	[SELECT FROM: Organizational personnel with incident handling responsibilities; organizational personnel with information security responsibilities].
	IR-04(03)-Test	[SELECT FROM: Mechanisms that support and/or implement continuity of operations].

IR-04(04)	INCIDENT HANDLING | INFORMATION CORRELATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-04(04)	incident information and individual incident responses are correlated to achieve an organization-wide perspective on incident awareness and response.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-04(04)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident handling; incident response plan; privacy plan; mechanisms supporting incident and event correlation; system design documentation; system configuration settings and associated documentation; system security plan; privacy plan; incident management correlation logs; event management correlation logs; security information and event management logs; incident management correlation reports; event management correlation reports; security information and event management reports; audit records; other relevant documents or records].
	IR-04(04)-Interview	[SELECT FROM: Organizational personnel with incident handling responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with whom incident information and individual incident responses are to be correlated].
	IR-04(04)-Test	[SELECT FROM: Organizational processes for correlating incident information and individual incident responses; mechanisms that support and or implement the correlation of incident response information with individual incident responses].

IR-04(05)	INCIDENT HANDLING | AUTOMATIC DISABLING OF SYSTEM	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-04(05)_ODP	***security violations that automatically disable a system are defined;***
	IR-04(05)	a configurable capability is implemented to automatically disable the system if ***<IR-04(05)_ODP security violations>*** are detected.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-04(05)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident handling; automated mechanisms supporting incident handling; system design documentation; system configuration settings and associated documentation; system security plan; incident response plan; privacy plan; other relevant documents or records].
	IR-04(05)-Interview	[SELECT FROM: Organizational personnel with incident handling responsibilities; organizational personnel with information security responsibilities; system developers].
	IR-04(05)-Test	[SELECT FROM: Incident handling capability for the organization; automated mechanisms supporting and/or implementing automatic disabling of the system].

IR-04(06)	INCIDENT HANDLING | INSIDER THREATS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-04(06)	an incident handling capability is implemented for incidents involving insider threats.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-04(06)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident handling; mechanisms supporting incident handling; system design documentation; system configuration settings and associated documentation; incident response plan; system security plan; audit records; other relevant documents or records].
	IR-04(06)-Interview	[SELECT FROM: Organizational personnel with incident handling responsibilities; organizational personnel with information security responsibilities].
	IR-04(06)-Test	[SELECT FROM: Incident handling capability for the organization].

IR-04(07)	INCIDENT HANDLING | INSIDER THREATS — INTRA-ORGANIZATION COORDINATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-04(07)_ODP	***entities that require coordination for an incident handling capability for insider threats are defined;***
	IR-04(07)[01]	an incident handling capability is coordinated for insider threats;
	IR-04(07)[02]	the coordinated incident handling capability includes ***<IR-04(07)_ODP entities>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-04(07)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident handling; incident response plan; insider threat program plan; insider threat CONOPS; system security plan; privacy plan; other relevant documents or records].
	IR-04(07)-Interview	[SELECT FROM: Organizational personnel with incident handling responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel/elements with whom the incident handling capability is to be coordinated].
	IR-04(07)-Test	[SELECT FROM: Organizational processes for coordinating incident handling].

IR-04(08)	INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-04(08)_ODP[01]	***external organizations with whom organizational incident information is to be coordinated and shared are defined;***
	IR-04(08)_ODP[02]	***incident information to be correlated and shared with organization-defined external organizations are defined;***

IR-04(08)	INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS	
	IR-04(08)	there is coordination with ***<IR-04(08)_ODP[01] external organizations>*** to correlate and share ***<IR-04(08)_ODP[02] incident information>*** to achieve a cross-organization perspective on incident awareness and more effective incident responses.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-04(08)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident handling; list of external organizations; records of incident handling coordination with external organizations; incident response plan; system security plan; privacy plan; other relevant documents or records].
	IR-04(08)-Interview	[SELECT FROM: Organizational personnel with incident handling responsibilities; organizational personnel with information security and privacy responsibilities; personnel from external organizations with whom incident response information is to be coordinated, shared, and correlated].
	IR-04(08)-Test	[SELECT FROM: Organizational processes for coordinating incident handling information with external organizations].

IR-04(09)	INCIDENT HANDLING | DYNAMIC RESPONSE CAPABILITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-04(09)_ODP	***dynamic response capabilities to be employed to respond to incidents are defined;***
	IR-04(09)	***<IR-04(09)_ODP dynamic response capabilities>*** are employed to respond to incidents.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-04(09)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident handling; automated mechanisms supporting dynamic response capabilities; system design documentation; system configuration settings and associated documentation; incident response plan; system security plan; audit records; other relevant documents or records].
	IR-04(09)-Interview	[SELECT FROM: Organizational personnel with incident handling responsibilities; organizational personnel with information security responsibilities].
	IR-04(09)-Test	[SELECT FROM: Organizational processes for dynamic response capability; automated mechanisms supporting and/or implementing the dynamic response capability for the organization].

IR-04(10)	INCIDENT HANDLING | SUPPLY CHAIN COORDINATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-04(10)	incident handling activities involving supply chain events are coordinated with other organizations involved in the supply chain.

IR-04(10)	INCIDENT HANDLING | SUPPLY CHAIN COORDINATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-04(10)-Examine	[SELECT FROM: Incident response policy; procedures addressing supply chain coordination and supply chain risk information sharing with the Federal Acquisition Security Council; acquisition contracts; service-level agreements; incident response plan; supply chain risk management plan; system security plan; incident response plans of other organization involved in supply chain activities; other relevant documents or records].
	IR-04(10)-Interview	[SELECT FROM: Organizational personnel with incident handling responsibilities; organizational personnel with mission and business responsibilities; organizational personnel with legal responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities; organizational personnel with acquisition responsibilities].

IR-04(11)	INCIDENT HANDLING | INTEGRATED INCIDENT RESPONSE TEAM	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-04(11)_ODP	***the time period within which an integrated incident response team can be deployed is defined;***
	IR-04(11)[01]	an integrated incident response team is established and maintained;
	IR-04(11)[02]	the integrated incident response team can be deployed to any location identified by the organization in ***<IR-04(11)_ODP time period>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-04(11)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident handling; procedures addressing incident response planning; incident response plan; system security plan; privacy plan; other relevant documents or records].
	IR-04(11)-Interview	[SELECT FROM: Organizational personnel with incident handling responsibilities; organizational personnel with information security and privacy responsibilities; members of the integrated incident response team].

IR-04(12)	INCIDENT HANDLING | MALICIOUS CODE AND FORENSIC ANALYSIS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-04(12)[01]	malicious code remaining in the system is analyzed after the incident;
	IR-04(12)[02]	other residual artifacts remaining in the system (if any) are analyzed after the incident.

IR-04(12)	INCIDENT HANDLING | MALICIOUS CODE AND FORENSIC ANALYSIS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-04(12)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident handling; procedures addressing code and forensic analysis; procedures addressing incident response; incident response plan; system design documentation; malicious code protection mechanisms, tools, and techniques; results from malicious code analyses; system security plan; system audit records; other relevant documents or records].
	IR-04(12)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel with responsibility for malicious code protection; organizational personnel responsible for incident response/management].
	IR-04(12)-Test	[SELECT FROM: Organizational process for incident response; organizational processes for conducting forensic analysis; tools and techniques for analysis of malicious code characteristics and behavior].

IR-04(13)	INCIDENT HANDLING | BEHAVIOR ANALYSIS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-04(13)_ODP	***environments or resources which may contain or may be related to anomalous or suspected adversarial behavior are defined;***
	IR-04(13)	anomalous or suspected adversarial behavior in or related to ***<IR-04(13)_ODP environments or resources>*** are analyzed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-04(13)-Examine	[SELECT FROM: Incident response policy; procedures addressing system monitoring tools and techniques; incident response plan; system monitoring logs or records; system monitoring tools and techniques documentation; system configuration settings and associated documentation; security plan; system component inventory; network diagram; system protocols documentation; list of acceptable thresholds for false positives and false negatives; system security plan; other relevant documents or records].
	IR-04(13)-Interview	[SELECT FROM: Organizational personnel with information security responsibilities; system/network administrators].
	IR-04(13)-Test	[SELECT FROM: Organizational processes for detecting anomalous behavior].

IR-04(14)	INCIDENT HANDLING | SECURITY OPERATIONS CENTER	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-04(14)[01]	a security operations center is established;
	IR-04(14)[02]	a security operations center is maintained.

IR-04(14)	INCIDENT HANDLING | SECURITY OPERATIONS CENTER	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-04(14)-Examine	[SELECT FROM: Incident response policy; contingency planning policy; procedures addressing incident handling; procedures addressing the security operations center operations; mechanisms supporting dynamic response capabilities; incident response plan; contingency plan; system security plan; other relevant documents or records].
	IR-04(14)-Interview	[SELECT FROM: Organizational personnel with incident handling responsibilities; organizational personnel with contingency planning responsibilities; security operations center personnel; organizational personnel with information security responsibilities].
	IR-04(14)-Test	[SELECT FROM: Mechanisms that support and/or implement the security operations center capability; mechanisms that support and/or implement the incident handling process].

IR-04(15)	INCIDENT HANDLING | PUBLIC RELATIONS AND REPUTATION REPAIR	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-04(15)(a)	public relations associated with an incident are managed;
	IR-04(15)(b)	measures are employed to repair the reputation of the organization.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-04(15)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident response; procedures addressing incident handling; incident response plan; system security plan; other relevant documents or records].
	IR-04(15)-Interview	[SELECT FROM: Organizational personnel with incident handling responsibilities; organizational personnel with information security responsibilities; organizational personnel with communications or public relations responsibilities].

IR-05	INCIDENT MONITORING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-05[01]	incidents are tracked;
	IR-05[02]	incidents are documented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-05-Examine	[SELECT FROM: Incident response policy; procedures addressing incident monitoring; incident response records and documentation; incident response plan; system security plan; privacy plan; other relevant documents or records].
	IR-05-Interview	[SELECT FROM: Organizational personnel with incident monitoring responsibilities; organizational personnel with information security and privacy responsibilities].

IR-05	INCIDENT MONITORING	
	IR-05-Test	[SELECT FROM: Incident monitoring capability for the organization; mechanisms supporting and/or implementing the tracking and documenting of system security incidents].

IR-05(01)	INCIDENT MONITORING | AUTOMATED TRACKING, DATA COLLECTION, AND ANALYSIS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-05(01)_ODP[01]	***automated mechanisms used to track incidents are defined;***
	IR-05(01)_ODP[02]	***automated mechanisms used to collect incident information are defined;***
	IR-05(01)_ODP[03]	***automated mechanisms used to analyze incident information are defined;***
	IR-05(01)[01]	incidents are tracked using ***<IR-05(01)_ODP[01] automated mechanisms>***;
	IR-05(01)[02]	incident information is collected using ***<IR-05(01)_ODP[02] automated mechanisms>***;
	IR-05(01)[03]	incident information is analyzed using ***<IR-05(01)_ODP[03] automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-05(01)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident monitoring; incident response records and documentation; system security plan; incident response plan; other relevant documents or records].
	IR-05(01)-Interview	[SELECT FROM: Organizational personnel with incident monitoring responsibilities; organizational personnel with information security responsibilities].
	IR-05(01)-Test	[SELECT FROM: Incident monitoring capability for the organization; automated mechanisms supporting and/or implementing the tracking and documenting of system security incidents].

IR-06	INCIDENT REPORTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-06_ODP[01]	***time period for personnel to report suspected incidents to the organizational incident response capability is defined;***
	IR-06_ODP[02]	***authorities to whom incident information is to be reported are defined;***
	IR-06a.	personnel is/are required to report suspected incidents to the organizational incident response capability within ***<IR-06_ODP[01] time period>***;
	IR-06b.	incident information is reported to ***<IR-06_ODP[02] authorities>***.

IR-06	INCIDENT REPORTING	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-06-Examine	[SELECT FROM: Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; incident response plan; system security plan; privacy plan; other relevant documents or records].
	IR-06-Interview	[SELECT FROM: Organizational personnel with incident reporting responsibilities; organizational personnel with information security and privacy responsibilities; personnel who have/should have reported incidents; personnel (authorities) to whom incident information is to be reported; system users].
	IR-06-Test	[SELECT FROM: Organizational processes for incident reporting; mechanisms supporting and/or implementing incident reporting].

IR-06(01)	INCIDENT REPORTING | AUTOMATED REPORTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-06(01)_ODP	***automated mechanisms used for reporting incidents are defined;***
	IR-06(01)	incidents are reported using ***<IR-06(01)_ODP automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-06(01)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident reporting; automated mechanisms supporting incident reporting; system design documentation; system configuration settings and associated documentation; incident response plan; system security plan; other relevant documents or records].
	IR-06(01)-Interview	[SELECT FROM: Organizational personnel with incident reporting responsibilities; organizational personnel with information security responsibilities].
	IR-06(01)-Test	[SELECT FROM: Organizational processes for incident reporting; automated mechanisms supporting and/or implementing the reporting of security incidents].

IR-06(02)	INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-06(02)_ODP	***personnel or roles to whom system vulnerabilities associated with reported incidents are reported to is/are defined;***
	IR-06(02)	system vulnerabilities associated with reported incidents are reported to ***<IR-06(02)_ODP personnel or roles>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-06(02)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident reporting; incident response plan; system security plan; privacy plan; security incident reports and associated system vulnerabilities; other relevant documents or records].

IR-06(02)	INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS	
	IR-06(02)-Interview	[SELECT FROM: Organizational personnel with incident reporting responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; personnel to whom vulnerabilities associated with security incidents are to be reported].
	IR-06(02)-Test	[SELECT FROM: Organizational processes for incident reporting; mechanisms supporting and/or implementing the reporting of vulnerabilities associated with security incidents].

IR-06(03)	INCIDENT REPORTING | SUPPLY CHAIN COORDINATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-06(03)	incident information is provided to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-06(03)-Examine	[SELECT FROM: Incident response policy; procedures addressing supply chain coordination and supply chain risk information sharing with the Federal Acquisition Security Council; acquisition policy; acquisition contracts; service-level agreements; incident response plan; supply chain risk management plan; system security plan; plans of other organizations involved in supply chain activities; other relevant documents or records].
	IR-06(03)-Interview	[SELECT FROM: Organizational personnel with incident reporting responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities; organization personnel with acquisition responsibilities].
	IR-06(03)-Test	[SELECT FROM: Organizational processes for incident reporting; organizational processes for supply chain risk information sharing; mechanisms supporting and/or implementing the reporting of incident information involved in the supply chain].

IR-07	INCIDENT RESPONSE ASSISTANCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-07[01]	an incident response support resource, integral to the organizational incident response capability, is provided;
	IR-07[02]	the incident response support resource offers advice and assistance to users of the system for the response and reporting of incidents.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-07-Examine	[SELECT FROM: Incident response policy; procedures addressing incident response assistance; incident response plan; system security plan; privacy plan; other relevant documents or records].

IR-07	INCIDENT RESPONSE ASSISTANCE	
	IR-07-Interview	[SELECT FROM: Organizational personnel with incident response assistance and support responsibilities; organizational personnel with access to incident response support and assistance capability; organizational personnel with information security and privacy responsibilities].
	IR-07-Test	[SELECT FROM: Organizational processes for incident response assistance; mechanisms supporting and/or implementing incident response assistance].

IR-07(01)	INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-07(01)_ODP	***automated mechanisms used to increase the availability of incident response information and support are defined;***
	IR-07(01)	the availability of incident response information and support is increased using ***<IR-07(01)_ODP automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-07(01)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident response assistance; automated mechanisms supporting incident response support and assistance; system design documentation; system configuration settings and associated documentation; incident response plan; system security plan; other relevant documents or records].
	IR-07(01)-Interview	[SELECT FROM: Organizational personnel with incident response support and assistance responsibilities; organizational personnel with access to incident response support and assistance capability; organizational personnel with information security responsibilities].
	IR-07(01)-Test	[SELECT FROM: Organizational processes for incident response assistance; automated mechanisms supporting and/or implementing an increase in the availability of incident response information and support].

IR-07(02)	INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-07(02)(a)	a direct, cooperative relationship is established between its incident response capability and external providers of the system protection capability;
	IR-07(02)(b)	organizational incident response team members are identified to the external providers.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-07(02)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident response assistance; incident response plan; system security plan; privacy plan; other relevant documents or records].

IR-07(02)	INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS	
	IR-07(02)-Interview	[SELECT FROM: Organizational personnel with incident response support and assistance responsibilities; external providers of system protection capability; organizational personnel with information security and privacy responsibilities].

IR-08	INCIDENT RESPONSE PLAN	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-08_ODP[01]	***personnel or roles that review and approve the incident response plan is/are identified;***
	IR-08_ODP[02]	***the frequency at which to review and approve the incident response plan is defined;***
	IR-08_ODP[03]	***entities, personnel, or roles with designated responsibility for incident response are defined;***
	IR-08_ODP[04]	***incident response personnel (identified by name and/or by role) to whom copies of the incident response plan are to be distributed is/are defined;***
	IR-08_ODP[05]	***organizational elements to which copies of the incident response plan are to be distributed are defined;***
	IR-08_ODP[06]	***incident response personnel (identified by name and/or by role) to whom changes to the incident response plan is/are communicated are defined;***
	IR-08_ODP[07]	***organizational elements to which changes to the incident response plan are communicated are defined;***
	IR-08a.01	an incident response plan is developed that provides the organization with a roadmap for implementing its incident response capability;
	IR-08a.02	an incident response plan is developed that describes the structure and organization of the incident response capability;
	IR-08a.03	an incident response plan is developed that provides a high-level approach for how the incident response capability fits into the overall organization;
	IR-08a.04	an incident response plan is developed that meets the unique requirements of the organization with regard to mission, size, structure, and functions;
	IR-08a.05	an incident response plan is developed that defines reportable incidents;
	IR-08a.06	an incident response plan is developed that provides metrics for measuring the incident response capability within the organization;
	IR-08a.07	an incident response plan is developed that defines the resources and management support needed to effectively maintain and mature an incident response capability;
	IR-08a.08	an incident response plan is developed that addresses the sharing of incident information;
	IR-08a.09	an incident response plan is developed that is reviewed and approved by ***<IR-08_ODP[01] personnel or roles> <IR-08_ODP[02] frequency>***;
	IR-08a.10	an incident response plan is developed that explicitly designates responsibility for incident response to ***<IR-08_ODP[03] entities, personnel, or roles>***.

IR-08	INCIDENT RESPONSE PLAN	
	IR-08b.[01]	copies of the incident response plan are distributed to ***<IR-08_ODP[04] incident response personnel>***;
	IR-08b.[02]	copies of the incident response plan are distributed to ***<IR-08_ODP[05] organizational elements>***;
	IR-08c.	the incident response plan is updated to address system and organizational changes or problems encountered during plan implementation, execution, or testing;
	IR-08d.[01]	incident response plan changes are communicated to ***<IR-08_ODP[06] incident response personnel>***;
	IR-08d.[02]	incident response plan changes are communicated to ***<IR-08_ODP[07] organizational elements>***;
	IR-08e.[01]	the incident response plan is protected from unauthorized disclosure;
	IR-08e.[02]	the incident response plan is protected from unauthorized modification.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-08-Examine	[SELECT FROM: Incident response policy; procedures addressing incident response planning; incident response plan; system security plan; privacy plan; records of incident response plan reviews and approvals; other relevant documents or records].
	IR-08-Interview	[SELECT FROM: Organizational personnel with incident response planning responsibilities; organizational personnel with information security and privacy responsibilities].
	IR-08-Test	[SELECT FROM: Organizational incident response plan and related organizational processes].

IR-08(01)	INCIDENT RESPONSE PLAN | BREACHES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-08(01)(a)	the incident response plan for breaches involving personally identifiable information includes a process to determine if notice to individuals or other organizations, including oversight organizations, is needed;
	IR-08(01)(b)	the incident response plan for breaches involving personally identifiable information includes an assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms;
	IR-08(01)(c)	the incident response plan for breaches involving personally identifiable information includes the identification of applicable privacy requirements.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-08(01)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident response planning; incident response plan; system security plan; privacy plan; records of incident response plan reviews and approvals; other relevant documents or records].

IR-08(01)	INCIDENT RESPONSE PLAN | BREACHES	
	IR-08(01)-Interview	[SELECT FROM: Organizational personnel with incident response planning responsibilities; organizational personnel with information security and privacy responsibilities].
	IR-08(01)-Test	[SELECT FROM: Organizational incident response plan and related organizational processes].

IR-09	INFORMATION SPILLAGE RESPONSE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-09_ODP[01]	***personnel or roles assigned the responsibility for responding to information spills is/are defined;***
	IR-09_ODP[02]	***personnel or roles to be alerted of the information spill using a method of communication not associated with the spill is/are defined;***
	IR-09_ODP[03]	***actions to be performed are defined;***
	IR-09a.	***<IR-09_ODP[01] personnel or roles>*** is/are assigned the responsibility to respond to information spills;
	IR-09b.	the specific information involved in the system contamination is identified in response to information spills;
	IR-09c.	***<IR-09_ODP[02] personnel or roles>*** is/are alerted of the information spill using a method of communication not associated with the spill;
	IR-09d.	the contaminated system or system component is isolated in response to information spills;
	IR-09e.	the information is eradicated from the contaminated system or component in response to information spills;
	IR-09f.	other systems or system components that may have been subsequently contaminated are identified in response to information spills;
	IR-09g.	***<IR-09_ODP[03] actions>*** are performed in response to information spills.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-09-Examine	[SELECT FROM: Incident response policy; procedures addressing information spillage; incident response plan; system security plan; records of information spillage alerts/notifications; list of personnel who should receive alerts of information spillage; list of actions to be performed regarding information spillage; other relevant documents or records].
	IR-09-Interview	[SELECT FROM: Organizational personnel with incident response responsibilities; organizational personnel with information security responsibilities].
	IR-09-Test	[SELECT FROM: Organizational processes for information spillage response; mechanisms supporting and/or implementing information spillage response actions and related communications].

IR-09(01)	INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL
	[WITHDRAWN: Incorporated into IR-09.]

IR-09(02)	INFORMATION SPILLAGE RESPONSE | TRAINING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-09(02)_ODP	***frequency at which to provide information spillage response training is defined;***
	IR-09(02)	information spillage response training is provided ***<IR-09(02)_ODP frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-09(02)-Examine	[SELECT FROM: Incident response policy; procedures addressing information spillage response training; information spillage response training curriculum; information spillage response training materials; incident response plan; system security plan; information spillage response training records; other relevant documents or records].
	IR-09(02)-Interview	[SELECT FROM: Organizational personnel with incident response training responsibilities; organizational personnel with information security responsibilities].

IR-09(03)	INFORMATION SPILLAGE RESPONSE | POST-SPILL OPERATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-09(03)_ODP	***procedures to be implemented to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions are defined;***
	IR-09(03)	***<IR-09(03)_ODP procedures>*** are implemented to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-09(03)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident response; procedures addressing information spillage; incident response plan; system security plan; other relevant documents or records].
	IR-09(03)-Interview	[SELECT FROM: Organizational personnel with incident response responsibilities; organizational personnel with information security responsibilities].
	IR-09(03)-Test	[SELECT FROM: Organizational processes for post-spill operations].

IR-09(04)	INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	IR-09(04)_ODP	***controls employed for personnel exposed to information not within assigned access authorizations are defined;***
	IR-09(04)	***<IR-09(04)_ODP controls>*** are employed for personnel exposed to information not within assigned access authorizations.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	IR-09(04)-Examine	[SELECT FROM: Incident response policy; procedures addressing incident response; procedures addressing information spillage; incident response plan; system security plan; security safeguards regarding information spillage/exposure to unauthorized personnel; other relevant documents or records].
	IR-09(04)-Interview	[SELECT FROM: Organizational personnel with incident response responsibilities; organizational personnel with information security responsibilities].
	IR-09(04)-Test	[SELECT FROM: Organizational processes for dealing with information exposed to unauthorized personnel; mechanisms supporting and/or implementing safeguards for personnel exposed to information not within assigned access authorizations].

IR-10	INTEGRATED INFORMATION SECURITY ANALYSIS TEAM
	[WITHDRAWN: Moved to IR-04(11).]

4.9 MAINTENANCE

MA-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-01_ODP[01]	***personnel or roles to whom the maintenance policy is to be disseminated is/are defined;***
	MA-01_ODP[02]	***personnel or roles to whom the maintenance procedures are to be disseminated is/are defined;***
	MA-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	MA-01_ODP[04]	***an official to manage the maintenance policy and procedures is defined;***
	MA-01_ODP[05]	***the frequency with which the current maintenance policy is reviewed and updated is defined;***
	MA-01_ODP[06]	***events that would require the current maintenance policy to be reviewed and updated are defined;***
	MA-01_ODP[07]	***the frequency with which the current maintenance procedures are reviewed and updated is defined;***
	MA-01_ODP[08]	***events that would require the maintenance procedures to be reviewed and updated are defined;***
	MA-01a.[01]	a maintenance policy is developed and documented;
	MA-01a.[02]	the maintenance policy is disseminated to ***<MA-01_ODP[01] personnel or roles>***;
	MA-01a.[03]	maintenance procedures to facilitate the implementation of the maintenance policy and associated maintenance controls are developed and documented;
	MA-01a.[04]	the maintenance procedures are disseminated to ***<MA-01_ODP[02] personnel or roles>***;
	MA-01a.01(a)[01]	the ***<MA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** maintenance policy addresses purpose;
	MA-01a.01(a)[02]	the ***<MA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** maintenance policy addresses scope;
	MA-01a.01(a)[03]	the ***<MA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** maintenance policy addresses roles;
	MA-01a.01(a)[04]	the ***<MA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** maintenance policy addresses responsibilities;
	MA-01a.01(a)[05]	the ***<MA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** maintenance policy addresses management commitment;
	MA-01a.01(a)[06]	the ***<MA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** maintenance policy addresses coordination among organizational entities;
	MA-01a.01(a)[07]	the ***<MA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** maintenance policy addresses compliance;

MA-01	POLICY AND PROCEDURES	
	MA-01a.01(b)	the ***<MA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** maintenance policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines;
	MA-01b.	the ***<MA-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the maintenance policy and procedures;
	MA-01c.01[01]	the current maintenance policy is reviewed and updated ***<MA-01_ODP[05] frequency>***;
	MA-01c.01[02]	the current maintenance policy is reviewed and updated following ***<MA-01_ODP[06] events>***;
	MA-01c.02[01]	the current maintenance procedures are reviewed and updated ***<MA-01_ODP[07] frequency>***;
	MA-01c.02[02]	the current maintenance procedures are reviewed and updated following ***<MA-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-01-Examine	[SELECT FROM: Maintenance policy and procedures; system security plan; privacy plan; organizational risk management strategy; other relevant documents or records].
	MA-01-Interview	[SELECT FROM: Organizational personnel with maintenance responsibilities; organizational personnel with information security and privacy responsibilities].

MA-02	CONTROLLED MAINTENANCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-02_ODP[01]	***personnel or roles required to explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance or repairs is/are defined;***
	MA-02_ODP[02]	***information to be removed from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement is defined;***
	MA-02_ODP[03]	***information to be included in organizational maintenance records is defined;***
	MA-02a.[01]	maintenance, repair, and replacement of system components are scheduled in accordance with manufacturer or vendor specifications and/or organizational requirements;
	MA-02a.[02]	maintenance, repair, and replacement of system components are documented in accordance with manufacturer or vendor specifications and/or organizational requirements;
	MA-02a.[03]	records of maintenance, repair, and replacement of system components are reviewed in accordance with manufacturer or vendor specifications and/or organizational requirements;
	MA-02b.[01]	all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location, are approved;

MA-02	CONTROLLED MAINTENANCE	
	MA-02b.[02]	all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location, are monitored;
	MA-02c.	***<MA-02_ODP[01] personnel or roles>*** is/are required to explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;
	MA-02d.	equipment is sanitized to remove ***<MA-02_ODP[02] information>*** from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement;
	MA-02e.	all potentially impacted controls are checked to verify that the controls are still functioning properly following maintenance, repair, or replacement actions;
	MA-02f.	***<MA-02_ODP[03] information>*** is included in organizational maintenance records.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-02-Examine	[SELECT FROM: Maintenance policy; procedures addressing controlled system maintenance; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; system security plan; other relevant documents or records].
	MA-02-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities; organizational personnel responsible for media sanitization; system/network administrators].
	MA-02-Test	[SELECT FROM: Organizational processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for the system; organizational processes for sanitizing system components; mechanisms supporting and/or implementing controlled maintenance; mechanisms implementing the sanitization of system components].

MA-02(01)	CONTROLLED MAINTENANCE | RECORD CONTENT	
	[WITHDRAWN: Incorporated into MA-02.]	

MA-02(02)	CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-02(02)_ODP[01]	***automated mechanisms used to schedule maintenance, repair, and replacement actions for the system are defined;***
	MA-02(02)_ODP[02]	***automated mechanisms used to conduct maintenance, repair, and replacement actions for the system are defined;***
	MA-02(02)_ODP[03]	***automated mechanisms used to document maintenance, repair, and replacement actions for the system are defined;***
	MA-02(02)(a)[01]	***<MA-02(02)_ODP[01] automated mechanisms>*** are used to schedule maintenance, repair, and replacement actions for the system;

MA-02(02)	CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES	
	MA-02(02)(a)[02]	***<MA-02(02)_ODP[02] automated mechanisms>*** are used to conduct maintenance, repair, and replacement actions for the system;
	MA-02(02)(a)[03]	***<MA-02(02)_ODP[03] automated mechanisms>*** are used to document maintenance, repair, and replacement actions for the system;
	MA-02(02)(b)[01]	up-to date, accurate, and complete records of all maintenance actions requested, scheduled, in process, and completed are produced.
	MA-02(02)(b)[02]	up-to date, accurate, and complete records of all repair actions requested, scheduled, in process, and completed are produced.
	MA-02(02)(b)[03]	up-to date, accurate, and complete records of all replacement actions requested, scheduled, in process, and completed are produced.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-02(02)-Examine	[SELECT FROM: Maintenance policy; procedures addressing controlled system maintenance; automated mechanisms supporting system maintenance activities; system configuration settings and associated documentation; maintenance records; system security plan; other relevant documents or records].
	MA-02(02)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	MA-02(02)-Test	[SELECT FROM: Automated mechanisms supporting and/or implementing controlled maintenance; automated mechanisms supporting and/or implementing the production of records of maintenance and repair actions].

MA-03	MAINTENANCE TOOLS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-03_ODP	***frequency at which to review previously approved system maintenance tools is defined;***
	MA-03a.[01]	the use of system maintenance tools is approved;
	MA-03a.[02]	the use of system maintenance tools is controlled;
	MA-03a.[03]	the use of system maintenance tools is monitored;
	MA-03b.	previously approved system maintenance tools are reviewed ***<MA-03_ODP frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-03-Examine	[SELECT FROM: Maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; maintenance records; system security plan; other relevant documents or records].
	MA-03-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities].

MA-03	MAINTENANCE TOOLS	
	MA-03-Test	[SELECT FROM: Organizational processes for approving, controlling, and monitoring maintenance tools; mechanisms supporting and/or implementing the approval, control, and/or monitoring of maintenance tools].

MA-03(01)	MAINTENANCE TOOLS | INSPECT TOOLS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-03(01)	maintenance tools used by maintenance personnel are inspected for improper or unauthorized modifications.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-03(01)-Examine	[SELECT FROM: Maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; maintenance tool inspection records; maintenance records; system security plan; other relevant documents or records].
	MA-03(01)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities].
	MA-03(01)-Test	[SELECT FROM: Organizational processes for inspecting maintenance tools; mechanisms supporting and/or implementing the inspection of maintenance tools].

MA-03(02)	MAINTENANCE TOOLS | INSPECT MEDIA	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-03(02)	media containing diagnostic and test programs are checked for malicious code before the media are used in the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-03(02)-Examine	[SELECT FROM: Maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; maintenance records; system security plan; other relevant documents or records].
	MA-03(02)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities].
	MA-03(02)-Test	[SELECT FROM: Organizational process for inspecting media for malicious code; mechanisms supporting and/or implementing the inspection of media used for maintenance].

MA-03(03)	MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-03(03)_ODP	***personnel or roles who can authorize removal of equipment from the facility is/ are defined;***
	MA-03(03)(a)	the removal of maintenance equipment containing organizational information is prevented by verifying that there is no organizational information contained on the equipment; or
	MA-03(03)(b)	the removal of maintenance equipment containing organizational information is prevented by sanitizing or destroying the equipment; or
	MA-03(03)(c)	the removal of maintenance equipment containing organizational information is prevented by retaining the equipment within the facility; or
	MA-03(03)(d)	the removal of maintenance equipment containing organizational information is prevented by obtaining an exemption from ***<MA-03(03)_ODP personnel or roles>*** explicitly authorizing removal of the equipment from the facility.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-03(03)-Examine	[SELECT FROM: Maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; maintenance records; equipment sanitization records; media sanitization records; exemptions for equipment removal; system security plan; other relevant documents or records].
	MA-03(03)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities; organizational personnel responsible for media sanitization].
	MA-03(03)-Test	[SELECT FROM: Organizational process for preventing unauthorized removal of information; mechanisms supporting media sanitization or destruction of equipment; mechanisms supporting verification of media sanitization].

MA-03(04)	MAINTENANCE TOOLS | RESTRICTED TOOL USE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-03(04)	the use of maintenance tools is restricted to authorized personnel only.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-03(04)-Examine	[SELECT FROM: Maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; list of personnel authorized to use maintenance tools; maintenance tool usage records; maintenance records; system security plan; other relevant documents or records].
	MA-03(04)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities].
	MA-03(04)-Test	[SELECT FROM: Organizational processes for restricting the use of maintenance tools; mechanisms supporting and/or implementing the restricted use of maintenance tools].

MA-03(05)	MAINTENANCE TOOLS | EXECUTION WITH PRIVILEGE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-03(05)	the use of maintenance tools that execute with increased privilege is monitored.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-03(05)-Examine	[SELECT FROM: Maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; list of personnel authorized to use maintenance tools; maintenance tool usage records; maintenance records; system security plan; other relevant documents or records].
	MA-03(05)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities].
	MA-03(05)-Test	[SELECT FROM: Organizational processes for restricting the use of maintenance tools; organizational process for monitoring maintenance tools and maintenance tool usage; mechanisms monitoring the use of maintenance tools].

MA-03(06)	MAINTENANCE TOOLS | SOFTWARE UPDATES AND PATCHES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-03(06)	maintenance tools are inspected to ensure that the latest software updates and patches are installed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-03(06)-Examine	[SELECT FROM: Maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; list of personnel authorized to use maintenance tools; maintenance tool usage records; maintenance records; system security plan; other relevant documents or records].
	MA-03(06)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities].
	MA-03(06)-Test	[SELECT FROM: Organizational processes for inspecting maintenance tools; organizational processes for maintenance tools updates; mechanisms supporting and/or implementing the inspection of maintenance tools; mechanisms supporting and/or implementing maintenance tool updates.].

MA-04	NONLOCAL MAINTENANCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-04a.[01]	nonlocal maintenance and diagnostic activities are approved;
	MA-04a.[02]	nonlocal maintenance and diagnostic activities are monitored;
	MA-04b.[01]	the use of nonlocal maintenance and diagnostic tools are allowed only as consistent with organizational policy;

MA-04	NONLOCAL MAINTENANCE	
	MA-04b.[02]	the use of nonlocal maintenance and diagnostic tools are documented in the security plan for the system;
	MA-04c.	strong authentication is employed in the establishment of nonlocal maintenance and diagnostic sessions;
	MA-04d.	records for nonlocal maintenance and diagnostic activities are maintained;
	MA-04e.[01]	session connections are terminated when nonlocal maintenance is completed;
	MA-04e.[02]	network connections are terminated when nonlocal maintenance is completed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-04-Examine	[SELECT FROM: Maintenance policy; procedures addressing nonlocal system maintenance; remote access policy; remote access procedures; system design documentation; system configuration settings and associated documentation; maintenance records; records of remote access; diagnostic records; system security plan; other relevant documents or records].
	MA-04-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	MA-04-Test	[SELECT FROM: Organizational processes for managing nonlocal maintenance; mechanisms implementing, supporting, and/or managing nonlocal maintenance; mechanisms for strong authentication of nonlocal maintenance diagnostic sessions; mechanisms for terminating nonlocal maintenance sessions and network connections].

MA-04(01)	NONLOCAL MAINTENANCE | LOGGING AND REVIEW	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-04(01)_ODP[01]	***audit events to be logged for nonlocal maintenance are defined;***
	MA-04(01)_ODP[02]	***audit events to be logged for diagnostic sessions are defined;***
	MA-04(01)(a)[01]	***<MA-04(01)_ODP[01] audit events>*** are logged for nonlocal maintenance sessions;
	MA-04(01)(a)[02]	***<MA-04(01)_ODP[02] audit events>*** are logged for nonlocal diagnostic sessions;
	MA-04(01)(b)[01]	the audit records of the maintenance sessions are reviewed to detect anomalous behavior;
	MA-04(01)(b)[02]	the audit records of the diagnostic sessions are reviewed to detect anomalous behavior.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-04(01)-Examine	[SELECT FROM: Maintenance policy; procedures addressing nonlocal system maintenance; list of audit events; system configuration settings and associated documentation; maintenance records; diagnostic records; audit records; reviews of maintenance and diagnostic session records; system security plan; other relevant documents or records].

MA-04(01)	NONLOCAL MAINTENANCE | LOGGING AND REVIEW	
	MA-04(01)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities; organizational personnel with audit and review responsibilities; system/network administrators].
	MA-04(01)-Test	[SELECT FROM: Organizational processes for audit and review of nonlocal maintenance; mechanisms supporting and/or implementing audit and review of nonlocal maintenance].

MA-04(02)	NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE	
	[WITHDRAWN: Incorporated into MA-01, MA-04.]	

MA-04(03)	NONLOCAL MAINTENANCE | COMPARABLE SECURITY AND SANITIZATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-04(03)(a)[01]	nonlocal maintenance services are required to be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced;
	MA-04(03)(a)[02]	nonlocal diagnostic services are required to be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or
	MA-04(03)(b)[01]	the component to be serviced is removed from the system prior to nonlocal maintenance or diagnostic services;
	MA-04(03)(b)[02]	the component to be serviced is sanitized (for organizational information);
	MA-04(03)(b)[03]	the component is inspected and sanitized (for potentially malicious software) after the service is performed and before reconnecting the component to the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-04(03)-Examine	[SELECT FROM: Maintenance policy; procedures addressing nonlocal system maintenance; service provider contracts and/or service-level agreements; maintenance records; inspection records; audit records; equipment sanitization records; media sanitization records; system security plan; other relevant documents or records].
	MA-04(03)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; system maintenance provider; organizational personnel with information security responsibilities; organizational personnel responsible for media sanitization; system/network administrators].
	MA-04(03)-Test	[SELECT FROM: Organizational processes for comparable security and sanitization for nonlocal maintenance; organizational processes for the removal, sanitization, and inspection of components serviced via nonlocal maintenance; mechanisms supporting and/or implementing component sanitization and inspection].

MA-04(04)	NONLOCAL MAINTENANCE | AUTHENTICATION AND SEPARATION OF MAINTENANCE SESSIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-04(04)_ODP	***authenticators that are replay resistant are defined;***
	MA-04(04)(a)	nonlocal maintenance sessions are protected by employing ***<MA-04(04)_ODP authenticators that are replay resistant>***;
	MA-04(04)(b)(01)	nonlocal maintenance sessions are protected by separating maintenance sessions from other network sessions with the system by physically separated communication paths; or
	MA-04(04)(b)(02)	nonlocal maintenance sessions are protected by logically separated communication paths.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-04(04)-Examine	[SELECT FROM: Maintenance policy; procedures addressing nonlocal system maintenance; system design documentation; system configuration settings and associated documentation; maintenance records; audit records; system security plan; other relevant documents or records].
	MA-04(04)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; network engineers; organizational personnel with information security responsibilities; system/network administrators].
	MA-04(04)-Test	[SELECT FROM: Organizational processes for protecting nonlocal maintenance sessions; mechanisms implementing replay-resistant authenticators; mechanisms implementing logically separated/encrypted communication paths].

MA-04(05)	NONLOCAL MAINTENANCE | APPROVALS AND NOTIFICATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-04(05)_ODP[01]	***personnel or roles required to approve each nonlocal maintenance session is/are defined;***
	MA-04(05)_ODP[02]	***personnel and roles to be notified of the date and time of planned nonlocal maintenance is/are defined;***
	MA-04(05)(a)	the approval of each nonlocal maintenance session is required by ***<MA-04(05)_ODP[01] personnel or roles>***;
	MA-04(05)(b)	***<MA-04(05)_ODP[02] personnel and roles>*** is/are notified of the date and time of planned nonlocal maintenance.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-04(05)-Examine	[SELECT FROM: Maintenance policy; procedures addressing nonlocal system maintenance; notifications supporting nonlocal maintenance sessions; maintenance records; audit records; system security plan; other relevant documents or records].

MA-04(05)	NONLOCAL MAINTENANCE | APPROVALS AND NOTIFICATIONS	
	MA-04(05)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with notification responsibilities; organizational personnel with approval responsibilities; organizational personnel with information security responsibilities].
	MA-04(05)-Test	[SELECT FROM: Organizational processes for approving and notifying personnel regarding nonlocal maintenance; mechanisms supporting the notification and approval of nonlocal maintenance].

MA-04(06)	NONLOCAL MAINTENANCE | CRYPTOGRAPHIC PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-04(06)_ODP	***cryptographic mechanisms to be implemented to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications are defined;***
	MA-04(06)[01]	***<MA-04(06)_ODP cryptographic mechanisms>*** are implemented to protect the integrity of nonlocal maintenance and diagnostic communications;
	MA-04(06)[02]	***<MA-04(06)_ODP cryptographic mechanisms>*** are implemented to protect the confidentiality of nonlocal maintenance and diagnostic communications.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-04(06)-Examine	[SELECT FROM: Maintenance policy; procedures addressing nonlocal system maintenance; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms protecting nonlocal maintenance activities; maintenance records; diagnostic records; audit records; system security plan; other relevant documents or records].
	MA-04(06)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; network engineers; organizational personnel with information security responsibilities; system/network administrators].
	MA-04(06)-Test	[SELECT FROM: Cryptographic mechanisms protecting nonlocal maintenance and diagnostic communications].

MA-04(07)	NONLOCAL MAINTENANCE | DISCONNECT VERIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-04(07)[01]	session connection termination is verified after the completion of nonlocal maintenance and diagnostic sessions;
	MA-04(07)[02]	network connection termination is verified after the completion of nonlocal maintenance and diagnostic sessions.

MA-04(07)	NONLOCAL MAINTENANCE | DISCONNECT VERIFICATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-04(07)-Examine	[SELECT FROM: Maintenance policy; procedures addressing nonlocal system maintenance; system design documentation; system configuration settings and associated documentation; session/network termination logs; cryptographic mechanisms protecting nonlocal maintenance activities; maintenance records; diagnostic records; audit records; system security plan; other relevant documents or records].
	MA-04(07)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; network engineers; organizational personnel with information security responsibilities; system/network administrators].
	MA-04(07)-Test	[SELECT FROM: Mechanisms implementing remote disconnect verifications of terminated nonlocal maintenance and diagnostic sessions].

MA-05	MAINTENANCE PERSONNEL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-05a.[01]	a process for maintenance personnel authorization is established;
	MA-05a.[02]	a list of authorized maintenance organizations or personnel is maintained;
	MA-05b.	non-escorted personnel performing maintenance on the system possess the required access authorizations;
	MA-05c.	organizational personnel with required access authorizations and technical competence is/are designated to supervise the maintenance activities of personnel who do not possess the required access authorizations.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-05-Examine	[SELECT FROM: Maintenance policy; procedures addressing maintenance personnel; service provider contracts; service-level agreements; list of authorized personnel; maintenance records; access control records; system security plan; other relevant documents or records].
	MA-05-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities].
	MA-05-Test	[SELECT FROM: Organizational processes for authorizing and managing maintenance personnel; mechanisms supporting and/or implementing authorization of maintenance personnel].

MA-05(01)	MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-05(01)_ODP	***alternate controls to be developed and implemented in the event that a system component cannot be sanitized, removed, or disconnected from the system are defined;***

MA-05(01)	MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS	
	MA-05(01)(a)(01)	procedures for the use of maintenance personnel who lack appropriate security clearances or are not U.S. citizens are implemented and include approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified escorting and supervising maintenance personnel without the needed access authorization during the performance of maintenance and diagnostic activities;
	MA-05(01)(a)(02)	procedures for the use of maintenance personnel who lack appropriate security clearances or are not U.S. citizens are implemented and include all volatile information storage components within the system being sanitized and all non-volatile storage media being removed or physically disconnected from the system and secured prior to initiating maintenance or diagnostic activities;
	MA-05(01)(b)	***<MA-05(01)_ODP alternate controls>*** are developed and implemented in the event that a system cannot be sanitized, removed, or disconnected from the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-05(01)-Examine	[SELECT FROM: Maintenance policy; procedures addressing maintenance personnel; system media protection policy; physical and environmental protection policy; list of maintenance personnel requiring escort/supervision; maintenance records; access control records; system security plan; other relevant documents or records].
	MA-05(01)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with personnel security responsibilities; organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities; organizational personnel responsible for media sanitization; system/network administrators].
	MA-05(01)-Test	[SELECT FROM: Organizational processes for managing maintenance personnel without appropriate access; mechanisms supporting and/or implementing alternative security safeguards; mechanisms supporting and/or implementing information storage component sanitization].

MA-05(02)	MAINTENANCE PERSONNEL | SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-05(02)[01]	personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information possess security clearances for at least the highest classification level and for compartments of information on the system;
	MA-05(02)[02]	personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information possess formal access approvals for at least the highest classification level and for compartments of information on the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-05(02)-Examine	[SELECT FROM: Maintenance policy; procedures addressing maintenance personnel; personnel records; maintenance records; access control records; access credentials; access authorizations; system security plan; other relevant documents or records].

MA-05(02)	MAINTENANCE PERSONNEL | SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS	
	MA-05(02)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with personnel security responsibilities; organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities].
	MA-05(02)-Test	[SELECT FROM: Organizational processes for managing security clearances for maintenance personnel].

MA-05(03)	MAINTENANCE PERSONNEL | CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-05(03)	personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information are U.S. citizens.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-05(03)-Examine	[SELECT FROM: Maintenance policy; procedures addressing maintenance personnel; personnel records; maintenance records; access control records; access credentials; access authorizations; system security plan; other relevant documents or records].
	MA-05(03)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with personnel security responsibilities; organizational personnel with information security responsibilities].

MA-05(04)	MAINTENANCE PERSONNEL | FOREIGN NATIONALS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-05(04)(a)	foreign nationals with appropriate security clearances are used to conduct maintenance and diagnostic activities on classified systems only when the systems are jointly owned and operated by the United States and foreign allied governments or owned and operated solely by foreign allied governments;
	MA-05(04)(b)[01]	approvals regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified systems are fully documented within Memoranda of Agreements;
	MA-05(04)(b)[02]	consents regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified systems are fully documented within Memoranda of Agreements;
	MA-05(04)(b)[03]	detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified systems are fully documented within Memoranda of Agreements.

MA-05(04)	MAINTENANCE PERSONNEL | FOREIGN NATIONALS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-05(04)-Examine	[SELECT FROM: Maintenance policy; procedures addressing maintenance personnel; system media protection policy; access control policy and procedures; physical and environmental protection policy and procedures; memorandum of agreement; maintenance records; access control records; access credentials; access authorizations; system security plan; other relevant documents or records].
	MA-05(04)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities, organizational personnel with personnel security responsibilities; organizational personnel managing memoranda of agreements; organizational personnel with information security responsibilities].
	MA-05(04)-Test	[SELECT FROM: Organizational processes for managing foreign national maintenance personnel].

MA-05(05)	MAINTENANCE PERSONNEL | NON-SYSTEM MAINTENANCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-05(05)	non-escorted personnel performing maintenance activities not directly associated with the system but in the physical proximity of the system have required access authorizations.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-05(05)-Examine	[SELECT FROM: Maintenance policy; procedures addressing maintenance personnel; system media protection policy; access control policy and procedures; physical and environmental protection policy and procedures; maintenance records; access control records; access authorizations; system security plan; other relevant documents or records].
	MA-05(05)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with personnel security responsibilities; organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities].

MA-06	TIMELY MAINTENANCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-06_ODP[01]	***system components for which maintenance support and/or spare parts are obtained are defined;***
	MA-06_ODP[02]	***time period within which maintenance support and/or spare parts are to be obtained after a failure are defined;***
	MA-06	maintenance support and/or spare parts are obtained for ***<MA-06_ODP[01] system components>*** within ***<MA-06_ODP[02] time period>*** of failure.

MA-06	TIMELY MAINTENANCE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-06-Examine	[SELECT FROM: Maintenance policy; procedures addressing system maintenance; service provider contracts; service-level agreements; inventory and availability of spare parts; system security plan; other relevant documents or records].
	MA-06-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with acquisition responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	MA-06-Test	[SELECT FROM: Organizational processes for ensuring timely maintenance].

MA-06(01)	TIMELY MAINTENANCE | PREVENTIVE MAINTENANCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-06(01)_ODP[01]	***system components on which preventive maintenance is to be performed are defined;***
	MA-06(01)_ODP[02]	***time intervals within which preventive maintenance is to be performed on system components are defined;***
	MA-06(01)	preventive maintenance is performed on ***<MA-06(01)_ODP[01] system components>*** at ***<MA-06(01)_ODP[02] time intervals>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-06(01)-Examine	[SELECT FROM: Maintenance policy; procedures addressing system maintenance; service provider contracts; service-level agreements; maintenance records; list of system components requiring preventive maintenance; system security plan; other relevant documents or records].
	MA-06(01)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	MA-06(01)-Test	[SELECT FROM: Organizational processes for preventive maintenance; mechanisms supporting and/or implementing preventive maintenance].

MA-06(02)	TIMELY MAINTENANCE | PREDICTIVE MAINTENANCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-06(02)_ODP[01]	***system components on which predictive maintenance is to be performed are defined;***
	MA-06(02)_ODP[02]	***time intervals within which predictive maintenance is to be performed are defined;***
	MA-06(02)	predictive maintenance is performed on ***<MA-06(02)_ODP[01] system components>*** at ***<MA-06(02)_ODP[02] time intervals>***.

MA-06(02)	TIMELY MAINTENANCE | PREDICTIVE MAINTENANCE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-06(02)-Examine	[SELECT FROM: Maintenance policy; procedures addressing system maintenance; service provider contracts; service-level agreements; maintenance records; list of system components requiring predictive maintenance; system security plan; other relevant documents or records].
	MA-06(02)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	MA-06(02)-Test	[SELECT FROM: Organizational processes for predictive maintenance; mechanisms supporting and/or implementing predictive maintenance].

MA-06(03)	TIMELY MAINTENANCE | AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-06(03)_ODP	***automated mechanisms used to transfer predictive maintenance data to a maintenance management system are defined;***
	MA-06(03)	predictive maintenance data is transferred to a maintenance management system using ***<MA-06(03)_ODP automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-06(03)-Examine	[SELECT FROM: Maintenance policy; procedures addressing system maintenance; service provider contracts; service-level agreements; maintenance records; list of system components requiring predictive maintenance; system security plan; other relevant documents or records].
	MA-06(03)-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	MA-06(03)-Test	[SELECT FROM: Automated mechanisms implementing the transfer of predictive maintenance data to a computerized maintenance management system; operations of the computer maintenance management system].

MA-07	FIELD MAINTENANCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MA-07_ODP[01]	***systems or system components on which field maintenance is restricted or prohibited to trusted maintenance facilities are defined;***
	MA-07_ODP[02]	***trusted maintenance facilities that are not restricted or prohibited from conducting field maintenance are defined;***
	MA-07	field maintenance on ***<MA-07_ODP[01] systems or system components>*** are restricted or prohibited to ***<MA-07_ODP[02] trusted maintenance facilities>***.

MA-07	FIELD MAINTENANCE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MA-07-Examine	[SELECT FROM: Maintenance policy; procedures addressing field maintenance; system design documentation; system configuration settings and associated documentation; maintenance records; diagnostic records; system security plan; other relevant documents or records.].
	MA-07-Interview	[SELECT FROM: Organizational personnel with system maintenance responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	MA-07-Test	[SELECT FROM: Organizational processes for managing field maintenance; mechanisms implementing, supporting, and/or managing field maintenance; mechanisms for strong authentication of field maintenance diagnostic sessions; mechanisms for terminating field maintenance sessions and network connections].

4.10 MEDIA PROTECTION

MP-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-01_ODP[01]	***personnel or roles to whom the media protection policy is to be disseminated is/are defined;***
	MP-01_ODP[02]	***personnel or roles to whom the media protection procedures are to be disseminated is/are defined;***
	MP-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	MP-01_ODP[04]	***an official to manage the media protection policy and procedures is defined;***
	MP-01_ODP[05]	***the frequency with which the current media protection policy is reviewed and updated is defined;***
	MP-01_ODP[06]	***events that would require the current media protection policy to be reviewed and updated are defined;***
	MP-01_ODP[07]	***the frequency with which the current media protection procedures are reviewed and updated is defined;***
	MP-01_ODP[08]	***events that would require media protection procedures to be reviewed and updated are defined;***
	MP-01a.[01]	a media protection policy is developed and documented;
	MP-01a.[02]	the media protection policy is disseminated to ***<MP-01_ODP[01] personnel or roles>***;
	MP-01a.[03]	media protection procedures to facilitate the implementation of the media protection policy and associated media protection controls are developed and documented;
	MP-01a.[04]	the media protection procedures are disseminated to ***<MP-01_ODP[02] personnel or roles>***;
	MP-01a.01(a)[01]	the ***<MP-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** media protection policy addresses purpose;
	MP-01a.01(a)[02]	the ***<MP-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** media protection policy addresses scope;
	MP-01a.01(a)[03]	the ***<MP-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** media protection policy addresses roles;
	MP-01a.01(a)[04]	the ***<MP-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** media protection policy addresses responsibilities;
	MP-01a.01(a)[05]	the ***<MP-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** media protection policy addresses management commitment;
	MP-01a.01(a)[06]	the ***<MP-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** media protection policy addresses coordination among organizational entities;
	MP-01a.01(a)[07]	the ***<MP-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** media protection policy compliance;

MP-01	POLICY AND PROCEDURES	
	MP-01a.01(b)	the media protection policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines;
	MP-01b.	the ***<MP-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the media protection policy and procedures.
	MP-01c.01[01]	the current media protection policy is reviewed and updated ***<MP-01_ODP[05] frequency>***;
	MP-01c.01[02]	the current media protection policy is reviewed and updated following ***<MP-01_ODP[06] events>***;
	MP-01c.02[01]	the current media protection procedures are reviewed and updated ***<MP-01_ODP[07] frequency>***;
	MP-01c.02[02]	the current media protection procedures are reviewed and updated following ***<MP-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-01-Examine	[SELECT FROM: Media protection policy and procedures; organizational risk management strategy; system security plan; privacy plan; other relevant documents or records].
	MP-01-Interview	[SELECT FROM: Organizational personnel with media protection responsibilities; organizational personnel with information security and privacy responsibilities].

MP-02	MEDIA ACCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-02_ODP[01]	***types of digital media to which access is restricted are defined;***
	MP-02_ODP[02]	***personnel or roles authorized to access digital media is/are defined;***
	MP-02_ODP[03]	***types of non-digital media to which access is restricted are defined;***
	MP-02_ODP[04]	***personnel or roles authorized to access non-digital media is/are defined;***
	MP-02[01]	access to ***<MP-02_ODP[01] types of digital media>*** is restricted to ***<MP-02_ODP[02] personnel or roles>***;
	MP-02[02]	access to ***<MP-02_ODP[03] types of non-digital media>*** is restricted to ***<MP-02_ODP[04] personnel or roles>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-02-Examine	[SELECT FROM: System media protection policy; procedures addressing media access restrictions; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control records; system security plan; other relevant documents or records].
	MP-02-Interview	[SELECT FROM: Organizational personnel with system media protection responsibilities; organizational personnel with information security responsibilities; system/network administrators].

MP-02	MEDIA ACCESS	
	MP-02-Test	[SELECT FROM: Organizational processes for restricting information media; mechanisms supporting and/or implementing media access restrictions].

MP-02(01)	MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS
	[WITHDRAWN: Incorporated into MP-04(02).]

MP-02(02)	MEDIA ACCESS | CRYPTOGRAPHIC PROTECTION
	[WITHDRAWN: Incorporated into SC-28(01).]

MP-03	MEDIA MARKING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-03_ODP[01]	***types of system media exempt from marking when remaining in controlled areas are defined;***
	MP-03_ODP[02]	***controlled areas where media is exempt from marking are defined;***
	MP-03a.	system media is marked to indicate distribution limitations, handling caveats, and applicable security markings (if any) of the information;
	MP-03b.	***<MP-03_ODP[01] types of media exempted from marking>*** remain within ***<MP-03_ODP[02] controlled areas>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-03-Examine	[SELECT FROM: System media protection policy; procedures addressing media marking; physical and environmental protection policy and procedures; list of system media marking security attributes; designated controlled areas; system security plan; other relevant documents or records].
	MP-03-Interview	[SELECT FROM: Organizational personnel with system media protection and marking responsibilities; organizational personnel with information security responsibilities].
	MP-03-Test	[SELECT FROM: Organizational processes for marking information media; mechanisms supporting and/or implementing media marking].

MP-04	MEDIA STORAGE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-04_ODP[01]	***types of digital media to be physically controlled are defined (if selected);***

MP-04	MEDIA STORAGE	
	MP-04_ODP[02]	***types of non-digital media to be physically controlled are defined (if selected);***
	MP-04_ODP[03]	***types of digital media to be securely stored are defined (if selected);***
	MP-04_ODP[04]	***types of non-digital media to be securely stored are defined (if selected);***
	MP-04_ODP[05]	***controlled areas within which to securely store digital media are defined;***
	MP-04_ODP[06]	***controlled areas within which to securely store non-digital media are defined;***
	MP-04a.[01]	***<MP-04_ODP[01] types of digital media>*** are physically controlled;
	MP-04a.[02]	***<MP-04_ODP[02] types of non-digital media>*** are physically controlled;
	MP-04a.[03]	***<MP-04_ODP[03] types of digital media>*** are securely stored within ***<MP-04_ODP[05] controlled areas>***;
	MP-04a.[04]	***<MP-04_ODP[04] types of non-digital media>*** are securely stored within ***<MP-04_ODP[06] controlled areas>***;
	MP-04b.	system media types (defined in MP-04_ODP[01], MP-04_ODP[02], MP-04_ODP[03], MP-04_ODP[04]) are protected until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-04-Examine	[SELECT FROM: System media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; system media; designated controlled areas; system security plan; other relevant documents or records].
	MP-04-Interview	[SELECT FROM: Organizational personnel with system media protection and storage responsibilities; organizational personnel with information security responsibilities].
	MP-04-Test	[SELECT FROM: Organizational processes for storing information media; mechanisms supporting and/or implementing secure media storage/media protection].

MP-04(01)	MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION
	[WITHDRAWN: Incorporated into SC-28(01).]

MP-04(02)	MEDIA STORAGE | AUTOMATED RESTRICTED ACCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-04(02)_ODP[01]	***automated mechanisms to restrict access to media storage areas are defined;***
	MP-04(02)_ODP[02]	***automated mechanisms to log access attempts to media storage areas are defined;***
	MP-04(02)_ODP[03]	***automated mechanisms to log access granted to media storage areas are defined;***

MP-04(02)	MEDIA STORAGE | AUTOMATED RESTRICTED ACCESS	
	MP-04(02)[01]	access to media storage areas is restricted using ***<MP-04(02)_ODP[01] automated mechanisms>***;
	MP-04(02)[02]	access attempts to media storage areas are logged using ***<MP-04(02)_ODP[02] automated mechanisms>***;
	MP-04(02)[03]	access granted to media storage areas is logged using ***<MP-04(02)_ODP[03] automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-04(02)-Examine	[SELECT FROM: System media protection policy; procedures addressing media storage; access control policy and procedures; physical and environmental protection policy and procedures; system design documentation; system configuration settings and associated documentation; media storage facilities; access control devices; access control records; audit records; system security plan; other relevant documents or records].
	MP-04(02)-Interview	[SELECT FROM: Organizational personnel with system media protection and storage responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	MP-04(02)-Test	[SELECT FROM: Automated mechanisms restricting access to media storage areas; automated mechanisms auditing access attempts and access granted to media storage areas].

MP-05	MEDIA TRANSPORT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-05_ODP[01]	***types of system media to protect and control during transport outside of controlled areas are defined;***
	MP-05_ODP[02]	***controls used to protect system media outside of controlled areas are defined;***
	MP-05_ODP[03]	***controls used to control system media outside of controlled areas are defined;***
	MP-05a.[01]	***<MP-05_ODP[01] types of system media>*** are protected during transport outside of controlled areas using ***<MP-05_ODP[02] controls>***;
	MP-05a.[02]	***<MP-05_ODP[01] types of system media>*** are controlled during transport outside of controlled areas using ***<MP-05_ODP[03] controls>***;
	MP-05b.	accountability for system media is maintained during transport outside of controlled areas;
	MP-05c.	activities associated with the transport of system media are documented;
	MP-05d.[01]	personnel authorized to conduct media transport activities is/are identified;
	MP-05d.[02]	activities associated with the transport of system media are restricted to identified authorized personnel.

MP-05	MEDIA TRANSPORT	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-05-Examine	[SELECT FROM: System media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; authorized personnel list; system media; designated controlled areas; system security plan; other relevant documents or records].
	MP-05-Interview	[SELECT FROM: Organizational personnel with system media protection and storage responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	MP-05-Test	[SELECT FROM: Organizational processes for storing information media; mechanisms supporting and/or implementing media storage/media protection].

MP-05(01)	MEDIA TRANSPORT | PROTECTION OUTSIDE OF CONTROLLED AREAS
	[WITHDRAWN: Incorporated into MP-05.]

MP-05(02)	MEDIA TRANSPORT | DOCUMENTATION OF ACTIVITIES
	[WITHDRAWN: Incorporated into MP-05.]

MP-05(03)	MEDIA TRANSPORT | CUSTODIANS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-05(03)[01]	a custodian to transport system media outside of controlled areas is identified;
	MP-05(03)[02]	the identified custodian is employed during the transport of system media outside of controlled areas.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-05(03)-Examine	[SELECT FROM: System media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; system media transport records; audit records; system security plan; other relevant documents or records].
	MP-05(03)-Interview	[SELECT FROM: Organizational personnel with system media transport responsibilities; organizational personnel with information security responsibilities].
	MP-05(03)-Test	[SELECT FROM: Organizational processes for identifying and employing a custodian to transport media outside of controlled areas].

MP-05(04)	MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION
	[WITHDRAWN: Incorporated into SC-28(01).]

MP-06	MEDIA SANITIZATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-06_ODP[01]	***system media to be sanitized prior to disposal is defined;***
	MP-06_ODP[02]	***system media to be sanitized prior to release from organizational control is defined;***
	MP-06_ODP[03]	***system media to be sanitized prior to release for reuse is defined;***
	MP-06_ODP[04]	***sanitization techniques and procedures to be used for sanitization prior to disposal are defined;***
	MP-06_ODP[05]	***sanitization techniques and procedures to be used for sanitization prior to release from organizational control are defined;***
	MP-06_ODP[06]	***sanitization techniques and procedures to be used for sanitization prior to release for reuse are defined;***
	MP-06a.[01]	***<MP-06_ODP[01] system media>*** is sanitized using ***<MP-06_ODP[04] sanitization techniques and procedures>*** prior to disposal;
	MP-06a.[02]	***<MP-06_ODP[02] system media>*** is sanitized using ***<MP-06_ODP[05] sanitization techniques and procedures>*** prior to release from organizational control;
	MP-06a.[03]	***<MP-06_ODP[03] system media>*** is sanitized using ***<MP-06_ODP[06] sanitization techniques and procedures>*** prior to release for reuse;
	MP-06b.	sanitization mechanisms with strength and integrity commensurate with the security category or classification of the information are employed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-06-Examine	[SELECT FROM: System media protection policy; procedures addressing media sanitization and disposal; applicable federal standards and policies addressing media sanitization policy; media sanitization records; system audit records; system design documentation; records retention and disposition policy; records retention and disposition procedures; system configuration settings and associated documentation; system security plan; privacy plan; other relevant documents or records].
	MP-06-Interview	[SELECT FROM: Organizational personnel with media sanitization responsibilities; organizational personnel with records retention and disposition responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	MP-06-Test	[SELECT FROM: Organizational processes for media sanitization; mechanisms supporting and/or implementing media sanitization].

MP-06(01)	MEDIA SANITIZATION | REVIEW, APPROVE, TRACK, DOCUMENT, AND VERIFY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-06(01)[01]	media sanitization and disposal actions are reviewed;
	MP-06(01)[02]	media sanitization and disposal actions are approved;
	MP-06(01)[03]	media sanitization and disposal actions are tracked;
	MP-06(01)[04]	media sanitization and disposal actions are documented;
	MP-06(01)[05]	media sanitization and disposal actions are verified.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-06(01)-Examine	[SELECT FROM: System media protection policy; procedures addressing media sanitization and disposal; records retention and disposition policy; records retention and disposition procedures; media sanitization and disposal records; review records for media sanitization and disposal actions; approvals for media sanitization and disposal actions; tracking records; verification records; system audit records; system security plan; privacy plan; other relevant documents or records].
	MP-06(01)-Interview	[SELECT FROM: Organizational personnel with system media sanitization and disposal responsibilities; organizational personnel with records retention and disposition responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators].
	MP-06(01)-Test	[SELECT FROM: Organizational processes for media sanitization; mechanisms supporting and/or implementing media sanitization; mechanisms supporting and/or implementing verification of media sanitization].

MP-06(02)	MEDIA SANITIZATION | EQUIPMENT TESTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-06(02)_ODP[01]	***frequency with which to test sanitization equipment is defined;***
	MP-06(02)_ODP[02]	***frequency with which to test sanitization procedures is defined;***
	MP-06(02)[01]	sanitization equipment is tested ***<MP-06(02)_ODP[01] frequency>*** to ensure that the intended sanitization is being achieved;
	MP-06(02)[02]	sanitization procedures are tested ***<MP-06(02)_ODP[02] frequency>*** to ensure that the intended sanitization is being achieved.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-06(02)-Examine	[SELECT FROM: System media protection policy; procedures addressing media sanitization and disposal; procedures addressing testing of media sanitization equipment; results of media sanitization equipment and procedures testing; system audit records; records retention and disposition policy; records retention and disposition procedures; system security plan; privacy plan; other relevant documents or records].

MP-06(02)	MEDIA SANITIZATION | EQUIPMENT TESTING	
	MP-06(02)-Interview	[SELECT FROM: Organizational personnel with system media sanitization responsibilities; organizational personnel with records retention and disposition responsibilities; organizational personnel with information security and privacy responsibilities].
	MP-06(02)-Test	[SELECT FROM: Organizational processes for media sanitization; automated mechanisms supporting and/or implementing media sanitization; automated mechanisms supporting and/or implementing media sanitization procedures; sanitization equipment].

MP-06(03)	MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-06(03)_ODP	***circumstances requiring sanitization of portable storage devices are defined;***
	MP-06(03)	non-destructive sanitization techniques are applied to portable storage devices prior to connecting such devices to the system under ***<MP-06(03)_ODP circumstances>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-06(03)-Examine	[SELECT FROM: System media protection policy; procedures addressing media sanitization and disposal; information on portable storage devices for the system; list of circumstances requiring sanitization of portable storage devices; media sanitization records; audit records; system security plan; other relevant documents or records].
	MP-06(03)-Interview	[SELECT FROM: Organizational personnel with system media sanitization responsibilities; organizational personnel with information security responsibilities].
	MP-06(03)-Test	[SELECT FROM: Organizational processes for media sanitization of portable storage devices; mechanisms supporting and/or implementing media sanitization].

MP-06(04)	MEDIA SANITIZATION | CONTROLLED UNCLASSIFIED INFORMATION
	[WITHDRAWN: Incorporated into MP-06.]

MP-06(05)	MEDIA SANITIZATION | CLASSIFIED INFORMATION
	[WITHDRAWN: Incorporated into MP-06.]

MP-06(06)	MEDIA SANITIZATION | MEDIA DESTRUCTION
	[WITHDRAWN: Incorporated into MP-06.]

MP-06(07)	MEDIA SANITIZATION | DUAL AUTHORIZATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-06(07)_ODP	***system media to be sanitized using dual authorization is defined;***
	MP-06(07)	dual authorization for sanitization of ***<MP-06(07)_ODP system media>*** is enforced.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-06(07)-Examine	[SELECT FROM: System media protection policy; procedures addressing media sanitization and disposal; dual authorization policy and procedures; list of system media requiring dual authorization for sanitization; authorization records; media sanitization records; audit records; system security plan; other relevant documents or records].
	MP-06(07)-Interview	[SELECT FROM: Organizational personnel with system media sanitization responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	MP-06(07)-Test	[SELECT FROM: Organizational processes requiring dual authorization for media sanitization; mechanisms supporting and/or implementing media sanitization; mechanisms supporting and/or implementing dual authorization].

MP-06(08)	MEDIA SANITIZATION | REMOTE PURGING OR WIPING OF INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-06(08)_ODP[01]	***systems or system components to purge or wipe information either remotely or under specific conditions are defined;***
	MP-06(08)_ODP[02]	***one of the following PARAMETER VALUES is selected: {remotely; under <MP-06(08)_ODP[03] conditions>};***
	MP-06(08)_ODP[03]	***conditions under which information is to be purged or wiped are defined (if selected);***
	MP-06(08)	the capability to purge or wipe information from ***<MP-06(08)_ODP[01] systems or system components> <MP-06(08)_ODP[02] SELECTED PARAMETER VALUE>*** is provided.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-06(08)-Examine	[SELECT FROM: System media protection policy; procedures addressing media sanitization and disposal; system design documentation; system configuration settings and associated documentation; authorization records; media sanitization records; audit records; system security plan; other relevant documents or records].
	MP-06(08)-Interview	[SELECT FROM: Organizational personnel with system media sanitization responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	MP-06(08)-Test	[SELECT FROM: Organizational processes for purging/wiping media; mechanisms supporting and/or implementing purge/wipe capabilities].

MP-07	MEDIA USE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-07_ODP[01]	***types of system media to be restricted or prohibited from use on systems or system components are defined;***
	MP-07_ODP[02]	***one of the following PARAMETER VALUES is selected: {restrict; prohibit};***
	MP-07_ODP[03]	***systems or system components on which the use of specific types of system media to be restricted or prohibited are defined;***
	MP-07_ODP[04]	***controls to restrict or prohibit the use of specific types of system media on systems or system components are defined;***
	MP-07a.	the use of ***<MP-07_ODP[01] types of system media>*** is ***<MP-07_ODP[02] SELECTED PARAMETER VALUE>*** on ***<MP-07_ODP[03] systems or system components>*** using ***<MP-07_ODP[04] controls>***;
	MP-07b.	the use of portable storage devices in organizational systems is prohibited when such devices have no identifiable owner.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-07-Examine	[SELECT FROM: System media protection policy; system use policy; procedures addressing media usage restrictions; rules of behavior; system design documentation; system configuration settings and associated documentation; audit records; system security plan; other relevant documents or records].
	MP-07-Interview	[SELECT FROM: Organizational personnel with system media use responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	MP-07-Test	[SELECT FROM: Organizational processes for media use; mechanisms restricting or prohibiting the use of system media on systems or system components].

MP-07(01)	MEDIA USE | PROHIBIT USE WITHOUT OWNER
	[WITHDRAWN: Incorporated into MP-07.]

MP-07(02)	MEDIA USE | PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-07(02)[01]	sanitization-resistant media is identified;
	MP-07(02)[02]	the use of sanitization-resistant media in organizational systems is prohibited.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-07(02)-Examine	[SELECT FROM: System media protection policy; system use policy; procedures addressing media usage restrictions; rules of behavior; system configuration settings and associated documentation; system security plan; other relevant documents or records].

MP-07(02)	MEDIA USE | PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA	
	MP-07(02)-Interview	[SELECT FROM: Organizational personnel with system media use responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	MP-07(02)-Test	[SELECT FROM: Organizational processes for media use; mechanisms prohibiting use of media on systems or system components].

MP-08	MEDIA DOWNGRADING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-08_ODP[01]	***a system media downgrading process is defined;***
	MP-08_ODP[02]	***system media requiring downgrading is defined;***
	MP-08a.[01]	a ***<MP-08_ODP[01] system media downgrading process>*** is established;
	MP-08a.[02]	the ***<MP-08_ODP[01] system media downgrading process>*** includes employing downgrading mechanisms with strength and integrity commensurate with the security category or classification of the information;
	MP-08b.[01]	there is verification that the system media downgrading process is commensurate with the security category and/or classification level of the information to be removed;
	MP-08b.[02]	there is verification that the system media downgrading process is commensurate with the access authorizations of the potential recipients of the downgraded information;
	MP-08c.	***<MP-08_ODP[02] system media requiring downgrading>*** is identified;
	MP-08d.	the identified system media is downgraded using the ***<MP-08_ODP[01] system media downgrading process>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-08-Examine	[SELECT FROM: System media protection policy; procedures addressing media downgrading; system categorization documentation; list of media requiring downgrading; records of media downgrading; audit records; system security plan; other relevant documents or records].
	MP-08-Interview	[SELECT FROM: Organizational personnel with system media downgrading responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	MP-08-Test	[SELECT FROM: Organizational processes for media downgrading; mechanisms supporting and/or implementing media downgrading].

MP-08(01)	MEDIA DOWNGRADING | DOCUMENTATION OF PROCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-08(01)	system media downgrading actions are documented.

MP-08(01)	MEDIA DOWNGRADING | DOCUMENTATION OF PROCESS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-08(01)-Examine	[SELECT FROM: System media protection policy; procedures addressing media downgrading; system categorization documentation; list of media requiring downgrading; records of media downgrading; audit records; system security plan; other relevant documents or records].
	MP-08(01)-Interview	[SELECT FROM: Organizational personnel with system media downgrading responsibilities; organizational personnel with information security responsibilities; system/network administrators].
	MP-08(01)-Test	[SELECT FROM: Organizational processes for media downgrading; mechanisms supporting and/or implementing media downgrading].

MP-08(02)	MEDIA DOWNGRADING | EQUIPMENT TESTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-08(02)_ODP[01]	***the frequency with which to test downgrading equipment is defined;***
	MP-08(02)_ODP[02]	***the frequency with which to test downgrading procedures is defined;***
	MP-08(02)[01]	downgrading equipment is tested ***<MP-08(02)_ODP[01] frequency>*** to ensure that downgrading actions are being achieved;
	MP-08(02)[02]	downgrading procedures are tested ***<MP-08(02)_ODP[02] frequency>*** to ensure that downgrading actions are being achieved.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-08(02)-Examine	[SELECT FROM: System media protection policy; procedures addressing media downgrading; procedures addressing testing of media downgrading equipment; results of downgrading equipment and procedures testing; records of media downgrading; audit records; system security plan; other relevant documents or records].
	MP-08(02)-Interview	[SELECT FROM: Organizational personnel with system media downgrading responsibilities; organizational personnel with information security responsibilities].
	MP-08(02)-Test	[SELECT FROM: Organizational processes for media downgrading; mechanisms supporting and/or implementing media downgrading].

MP-08(03)	MEDIA DOWNGRADING | CONTROLLED UNCLASSIFIED INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-08(03)[01]	system media containing controlled unclassified information is identified;
	MP-08(03)[02]	system media containing controlled unclassified information is downgraded prior to public release.

MP-08(03)	MEDIA DOWNGRADING | CONTROLLED UNCLASSIFIED INFORMATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-08(03)-Examine	[SELECT FROM: System media protection policy; access authorization policy; procedures addressing downgrading of media containing CUI; applicable federal and organizational standards and policies regarding protection of CUI; media downgrading records; system security plan; other relevant documents or records].
	MP-08(03)-Interview	[SELECT FROM: Organizational personnel with system media downgrading responsibilities; organizational personnel with information security responsibilities].
	MP-08(03)-Test	[SELECT FROM: Organizational processes for media downgrading; mechanisms supporting and/or implementing media downgrading].

MP-08(04)	MEDIA DOWNGRADING | CLASSIFIED INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	MP-08(04)[01]	system media containing classified information is identified;
	MP-08(04)[02]	system media containing classified information is downgraded prior to release to individuals without required access authorizations.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	MP-08(04)-Examine	[SELECT FROM: System media protection policy; access authorization policy; procedures addressing downgrading of media containing classified information; procedures addressing handling of classified information; NSA standards and policies regarding protection of classified information; media downgrading records; system security plan; other relevant documents or records].
	MP-08(04)-Interview	[SELECT FROM: Organizational personnel with system media downgrading responsibilities; organizational personnel with information security responsibilities].
	MP-08(04)-Test	[SELECT FROM: Organizational processes for media downgrading; mechanisms supporting and/or implementing media downgrading].

4.11 PHYSICAL AND ENVIRONMENTAL PROTECTION

PE-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-01_ODP[01]	***personnel or roles to whom the physical and environmental protection policy is to be disseminated is/are defined;***
	PE-01_ODP[02]	***personnel or roles to whom the physical and environmental protection procedures are to be disseminated is/are defined;***
	PE-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	PE-01_ODP[04]	***an official to manage the physical and environmental protection policy and procedures is defined;***
	PE-01_ODP[05]	***the frequency at which the current physical and environmental protection policy is reviewed and updated is defined;***
	PE-01_ODP[06]	***events that would require the current physical and environmental protection policy to be reviewed and updated are defined;***
	PE-01_ODP[07]	***the frequency at which the current physical and environmental protection procedures are reviewed and updated is defined;***
	PE-01_ODP[08]	***events that would require the physical and environmental protection procedures to be reviewed and updated are defined;***
	PE-01a.[01]	a physical and environmental protection policy is developed and documented;
	PE-01a.[02]	the physical and environmental protection policy is disseminated to ***<PE-01_ODP[01] personnel or roles>***;
	PE-01a.[03]	physical and environmental protection procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls are developed and documented;
	PE-01a.[04]	the physical and environmental protection procedures are disseminated to ***<PE-01_ODP[02] personnel or roles>***;
	PE-01a.01(a)[01]	the ***<PE-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** physical and environmental protection policy addresses purpose;
	PE-01a.01(a)[02]	the ***<PE-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** physical and environmental protection policy addresses scope;
	PE-01a.01(a)[03]	the ***<PE-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** physical and environmental protection policy addresses roles;
	PE-01a.01(a)[04]	the ***<PE-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** physical and environmental protection policy addresses responsibilities;
	PE-01a.01(a)[05]	the ***<PE-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** physical and environmental protection policy addresses management commitment;
	PE-01a.01(a)[06]	the ***<PE-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** physical and environmental protection policy addresses coordination among organizational entities;

PE-01	POLICY AND PROCEDURES	
	PE-01a.01(a)[07]	the ***<PE-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** physical and environmental protection policy addresses compliance;
	PE-01a.01(b)	the ***<PE-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** physical and environmental protection policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines;
	PE-01b.	the ***<PE-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures;
	PE-01c.01[01]	the current physical and environmental protection policy is reviewed and updated ***<PE-01_ODP[05] frequency>***;
	PE-01c.01[02]	the current physical and environmental protection policy is reviewed and updated following ***<PE-01_ODP[06] events>***;
	PE-01c.02[01]	the current physical and environmental protection procedures are reviewed and updated ***<PE-01_ODP[07] frequency>***;
	PE-01c.02[02]	the current physical and environmental protection procedures are reviewed and updated following ***<PE-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-01-Examine	[SELECT FROM: Physical and environmental protection policy and procedures; system security plan; privacy plan; organizational risk management strategy; other relevant documents or records].
	PE-01-Interview	[SELECT FROM: Organizational personnel with physical and environmental protection responsibilities; organizational personnel with information security and privacy responsibilities].

PE-02	PHYSICAL ACCESS AUTHORIZATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-02_ODP	***frequency at which to review the access list detailing authorized facility access by individuals is defined;***
	PE-02a.[01]	a list of individuals with authorized access to the facility where the system resides has been developed;
	PE-02a.[02]	the list of individuals with authorized access to the facility where the system resides has been approved;
	PE-02a.[03]	the list of individuals with authorized access to the facility where the system resides has been maintained;
	PE-02b.	authorization credentials are issued for facility access;
	PE-02c.	the access list detailing authorized facility access by individuals is reviewed ***<PE-02_ODP frequency>***;
	PE-02d.	individuals are removed from the facility access list when access is no longer required.

PE-02	PHYSICAL ACCESS AUTHORIZATIONS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-02-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; physical access list reviews; physical access termination records and associated documentation; system security plan; other relevant documents or records].
	PE-02-Interview	[SELECT FROM: Organizational personnel with physical access authorization responsibilities; organizational personnel with physical access to system facility; organizational personnel with information security responsibilities].
	PE-02-Test	[SELECT FROM: Organizational processes for physical access authorizations; mechanisms supporting and/or implementing physical access authorizations].

PE-02(01)	PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION OR ROLE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-02(01)	physical access to the facility where the system resides is authorized based on position or role.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-02(01)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access authorizations; physical access control logs or records; list of positions/roles and corresponding physical access authorizations; system entry and exit points; system security plan; other relevant documents or records].
	PE-02(01)-Interview	[SELECT FROM: Organizational personnel with physical access authorization responsibilities; organizational personnel with physical access to system facility; organizational personnel with information security responsibilities].
	PE-02(01)-Test	[SELECT FROM: Organizational processes for physical access authorizations; mechanisms supporting and/or implementing physical access authorizations].

PE-02(02)	PHYSICAL ACCESS AUTHORIZATIONS | TWO FORMS OF IDENTIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-02(02)_ODP	***a list of acceptable forms of identification for visitor access to the facility where the system resides is defined;***
	PE-02(02)	two forms of identification are required from ***<PE-02(02)_ODP list of acceptable forms of identification>*** for visitor access to the facility where the system resides.

PE-02(02)	PHYSICAL ACCESS AUTHORIZATIONS | TWO FORMS OF IDENTIFICATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-02(02)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access authorizations; list of acceptable forms of identification for visitor access to the facility where the system resides; access authorization forms; access credentials; physical access control logs or records; system security plan; other relevant documents or records].
	PE-02(02)-Interview	[SELECT FROM: Organizational personnel with physical access authorization responsibilities; organizational personnel with physical access to the system facility; organizational personnel with information security responsibilities].
	PE-02(02)-Test	[SELECT FROM: Organizational processes for physical access authorizations; mechanisms supporting and/or implementing physical access authorizations].

PE-02(03)	PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-02(03)_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system; <PE-02(03)_ODP[02] physical access authorizations>};***
	PE-02(03)_ODP[02]	***physical access authorizations for unescorted access to the facility where the system resides are defined (if selected);***
	PE-02(03)	unescorted access to the facility where the system resides is restricted to personnel with ***<PE-02(03)_ODP[01] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-02(03)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; security clearances; access authorizations; access credentials; physical access control logs or records; system security plan; other relevant documents or records].
	PE-02(03)-Interview	[SELECT FROM: Organizational personnel with physical access authorization responsibilities; organizational personnel with physical access to the system facility; organizational personnel with information security responsibilities].
	PE-02(03)-Test	[SELECT FROM: Organizational processes for physical access authorizations; mechanisms supporting and/or implementing physical access authorizations].

PE-03	PHYSICAL ACCESS CONTROL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-03_ODP[01]	***entry and exit points to the facility in which the system resides are defined;***

PE-03	PHYSICAL ACCESS CONTROL	
	PE-03_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {<PE-03_ODP[03] systems or devices>; guards};***
	PE-03_ODP[03]	***physical access control systems or devices used to control ingress and egress to the facility are defined (if selected);***
	PE-03_ODP[04]	***entry or exit points for which physical access logs are maintained are defined;***
	PE-03_ODP[05]	***physical access controls to control access to areas within the facility designated as publicly accessible are defined;***
	PE-03_ODP[06]	***circumstances requiring visitor escorts and control of visitor activity are defined;***
	PE-03_ODP[07]	***physical access devices to be inventoried are defined;***
	PE-03_ODP[08]	***frequency at which to inventory physical access devices is defined;***
	PE-03_ODP[09]	***frequency at which to change combinations is defined;***
	PE-03_ODP[10]	***frequency at which to change keys is defined;***
	PE-03a.01	physical access authorizations are enforced at ***<PE-03_ODP[01] entry and exit points>*** by verifying individual access authorizations before granting access to the facility;
	PE-03a.02	physical access authorizations are enforced at ***<PE-03_ODP[01] entry and exit points>*** by controlling ingress and egress to the facility using ***<PE-03_ODP[02] SELECTED PARAMETER VALUE(S)>***;
	PE-03b.	physical access audit logs are maintained for ***<PE-03_ODP[04] entry or exit points>***;
	PE-03c.	access to areas within the facility designated as publicly accessible are maintained by implementing ***<PE-03_ODP[05] physical access controls>***;
	PE-03d.[01]	visitors are escorted;
	PE-03d.[02]	visitor activity is controlled ***<PE-03_ODP[06] circumstances>***;
	PE-03e.[01]	keys are secured;
	PE-03e.[02]	combinations are secured;
	PE-03e.[03]	other physical access devices are secured;
	PE-03f.	***<PE-03_ODP[07] physical access devices>*** are inventoried ***<PE-03_ODP[08] frequency>***;
	PE-03g.[01]	combinations are changed ***<PE-03_ODP[09] frequency>*** , when combinations are compromised, or when individuals possessing the combinations are transferred or terminated;
	PE-03g.[02]	keys are changed ***<PE-03_ODP[10] frequency>*** , when keys are lost, or when individuals possessing the keys are transferred or terminated.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-03-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; system security plan; other relevant documents or records].

PE-03	PHYSICAL ACCESS CONTROL	
	PE-03-Interview	[SELECT FROM: Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities].
	PE-03-Test	[SELECT FROM: Organizational processes for physical access control; mechanisms supporting and/or implementing physical access control; physical access control devices].

PE-03(01)	PHYSICAL ACCESS CONTROL | SYSTEM ACCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-03(01)_ODP	***physical spaces containing one or more components of the system are defined;***
	PE-03(01)[01]	physical access authorizations to the system are enforced;
	PE-03(01)02]	physical access controls are enforced for the facility at ***<PE-03(01)_ODP physical spaces>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-03(01)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; physical access control devices; access authorizations; access credentials; system entry and exit points; list of areas within the facility containing concentrations of system components or system components requiring additional physical protection; system security plan; other relevant documents or records].
	PE-03(01)-Interview	[SELECT FROM: Organizational personnel with physical access authorization responsibilities; organizational personnel with information security responsibilities].
	PE-03(01)-Test	[SELECT FROM: Organizational processes for physical access control to the information system/components; mechanisms supporting and/or implementing physical access control for facility areas containing system components].

PE-03(02)	PHYSICAL ACCESS CONTROL | FACILITY AND SYSTEMS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-03(02)_ODP	***the frequency at which to perform security checks at the physical perimeter of the facility or system for exfiltration of information or removal of system components is defined;***
	PE-03(02)	security checks are performed ***<PE-03(02)_ODP frequency>*** at the physical perimeter of the facility or system for exfiltration of information or removal of system components.

PE-03(02)	PHYSICAL ACCESS CONTROL | FACILITY AND SYSTEMS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-03(02)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; records of security checks; security audit reports; security inspection reports; facility layout documentation; system entry and exit points; system security plan; other relevant documents or records].
	PE-03(02)-Interview	[SELECT FROM: Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities].
	PE-03(02)-Test	[SELECT FROM: Organizational processes for physical access control to the facility and/or system; mechanisms supporting and/or implementing physical access control for the facility or system; mechanisms supporting and/or implementing security checks for the unauthorized exfiltration of information].

PE-03(03)	PHYSICAL ACCESS CONTROL | CONTINUOUS GUARDS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-03(03)_ODP	***physical access points to the facility where the system resides are defined;***
	PE-03(03)	guards are employed to control ***<PE-03(03)_ODP physical access points>*** to the facility where the system resides 24 hours per day, 7 days per week.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-03(03)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; physical access control logs or records; physical access control devices; facility surveillance records; facility layout documentation; system entry and exit points; system security plan; other relevant documents or records].
	PE-03(03)-Interview	[SELECT FROM: Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities].
	PE-03(03)-Test	[SELECT FROM: Organizational processes for physical access control to the facility where the system resides; mechanisms supporting and/or implementing physical access control for the facility where the system resides].

PE-03(04)	PHYSICAL ACCESS CONTROL | LOCKABLE CASINGS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-03(04)_ODP	***system components to be protected from unauthorized physical access are defined;***
	PE-03(04)	lockable physical casings are used to protect ***<PE-03(04)_ODP system components>*** from unauthorized access.

PE-03(04)	PHYSICAL ACCESS CONTROL | LOCKABLE CASINGS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-03(04)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; list of system components requiring protection through lockable physical casings; lockable physical casings; system security plan; other relevant documents or records].
	PE-03(04)-Interview	[SELECT FROM: Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities].
	PE-03(04)-Test	[SELECT FROM: Lockable physical casings].

PE-03(05)	PHYSICAL ACCESS CONTROL | TAMPER PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-03(05)_ODP[01]	***anti-tamper technologies to be employed are defined;***
	PE-03(05)_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {detect; prevent};***
	PE-03(05)_ODP[03]	***hardware components to be protected from physical tampering or alteration are defined;***
	PE-03(05)	***<PE-03(05)_ODP[01] anti-tamper technologies>*** are employed to ***<PE-03(05)_ODP[02] SELECTED PARAMETER VALUE(S)>*** physical tampering or alteration of ***<PE-03(05)_ODP[03] hardware components>*** within the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-03(05)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; list of security safeguards to detect/prevent physical tampering or alteration of system hardware components; system security plan; other relevant documents or records].
	PE-03(05)-Interview	[SELECT FROM: Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities].
	PE-03(05)-Test	[SELECT FROM: Organizational processes to detect/prevent physical tampering or alteration of system hardware components; mechanisms/security safeguards supporting and/or implementing the detection/prevention of physical tampering/ alternation of system hardware components].

PE-03(06)	PHYSICAL ACCESS CONTROL | FACILITY PENETRATION TESTING
	[WITHDRAWN: Incorporated into CA-08.]

PE-03(07)	PHYSICAL ACCESS CONTROL | PHYSICAL BARRIERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-03(07)	physical barriers are used to limit access.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-03(07)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; list of physical barriers to limit access to the system; system security plan; other relevant documents or records].
	PE-03(07)-Interview	[SELECT FROM: Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities].

PE-03(08)	PHYSICAL ACCESS CONTROL | ACCESS CONTROL VESTIBULES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-03(08)_ODP	***locations within the facility where access control vestibules are to be employed are defined;***
	PE-03(08)	access control vestibules are employed at ***<PE-03(08)_ODP locations>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-03(08)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; list of access control vestibules and locations; system security plan; other relevant documents or records].
	PE-03(08)-Interview	[SELECT FROM: Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities].
	PE-03(08)-Test	[SELECT FROM: Organizational processes for vestibules to prevent unauthorized access.].

PE-04	ACCESS CONTROL FOR TRANSMISSION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-04_ODP[01]	***system distribution and transmission lines requiring physical access controls are defined;***
	PE-04_ODP[02]	***security controls to be implemented to control physical access to system distribution and transmission lines within the organizational facility are defined;***
	PE-04	physical access to ***<PE-04_ODP[01] system distribution and transmission lines>*** within organizational facilities is controlled using ***<PE-04_ODP[02] security controls>***.

PE-04	ACCESS CONTROL FOR TRANSMISSION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-04-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing access control for transmission mediums; system design documentation; facility communications and wiring diagrams; list of physical security safeguards applied to system distribution and transmission lines; system security plan; other relevant documents or records].
	PE-04-Interview	[SELECT FROM: Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities].
	PE-04-Test	[SELECT FROM: Organizational processes for access control to distribution and transmission lines; mechanisms/security safeguards supporting and/or implementing access control to distribution and transmission lines].

PE-05	ACCESS CONTROL FOR OUTPUT DEVICES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-05_ODP	***output devices that require physical access control to output are defined;***
	PE-05	physical access to output from ***<PE-05_ODP output devices>*** is controlled to prevent unauthorized individuals from obtaining the output.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-05-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing access control for display medium; facility layout of system components; actual displays from system components; list of output devices and associated outputs requiring physical access controls; physical access control logs or records for areas containing output devices and related outputs; system security plan; other relevant documents or records].
	PE-05-Interview	[SELECT FROM: Organizational personnel with physical access control responsibilities; organizational personnel with information security responsibilities].
	PE-05-Test	[SELECT FROM: Organizational processes for access control to output devices; mechanisms supporting and/or implementing access control to output devices].

PE-05(01)	ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS
	[WITHDRAWN: Incorporated into PE-05.]

PE-05(02)	ACCESS CONTROL FOR OUTPUT DEVICES | LINK TO INDIVIDUAL IDENTITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-05(02)	individual identity is linked to the receipt of output from output devices.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-05(02)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access control; system design documentation; system configuration settings and associated documentation; list of output devices and associated outputs requiring physical access controls; physical access control logs or records for areas containing output devices and related outputs; system audit records; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	PE-05(02)-Interview	[SELECT FROM: Organizational personnel with physical access control responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; system developers].
	PE-05(02)-Test	[SELECT FROM: Organizational processes for access control to output devices; mechanisms supporting and/or implementing access control to output devices].

PE-05(03)	ACCESS CONTROL FOR OUTPUT DEVICES | MARKING OUTPUT DEVICES
	[WITHDRAWN: Incorporated into PE-22.]

PE-06	MONITORING PHYSICAL ACCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-06_ODP[01]	***the frequency at which to review physical access logs is defined;***
	PE-06_ODP[02]	***events or potential indication of events requiring physical access logs to be reviewed are defined;***
	PE-06a.	physical access to the facility where the system resides is monitored to detect and respond to physical security incidents;
	PE-06b.[01]	physical access logs are reviewed ***<PE-06_ODP[01] frequency>***;
	PE-06b.[02]	physical access logs are reviewed upon occurrence of ***<PE-06_ODP[02] events>***;
	PE-06c.[01]	results of reviews are coordinated with organizational incident response capabilities;
	PE-06c.[02]	results of investigations are coordinated with organizational incident response capabilities.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-06-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access monitoring; physical access logs or records; physical access monitoring records; physical access log reviews; system security plan; other relevant documents or records].

PE-06	MONITORING PHYSICAL ACCESS	
	PE-06-Interview	[SELECT FROM: Organizational personnel with physical access monitoring responsibilities; organizational personnel with incident response responsibilities; organizational personnel with information security responsibilities].
	PE-06-Test	[SELECT FROM: Organizational processes for monitoring physical access; mechanisms supporting and/or implementing physical access monitoring; mechanisms supporting and/or implementing the review of physical access logs].

PE-06(01)	MONITORING PHYSICAL ACCESS | INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-06(01)[01]	physical access to the facility where the system resides is monitored using physical intrusion alarms;
	PE-06(01)[02]	physical access to the facility where the system resides is monitored using physical surveillance equipment.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-06(01)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access monitoring; physical access logs or records; physical access monitoring records; physical access log reviews; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	PE-06(01)-Interview	[SELECT FROM: Organizational personnel with physical access monitoring responsibilities; organizational personnel with incident response responsibilities; organizational personnel with information security and privacy responsibilities].
	PE-06(01)-Test	[SELECT FROM: Organizational processes for monitoring physical intrusion alarms and surveillance equipment; mechanisms supporting and/or implementing physical access monitoring; mechanisms supporting and/or implementing physical intrusion alarms and surveillance equipment].

PE-06(02)	MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION AND RESPONSES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-06(02)_ODP[01]	***classes or types of intrusions to be recognized by automated mechanisms are defined;***
	PE-06(02)_ODP[02]	***response actions to be initiated by automated mechanisms when organization-defined classes or types of intrusions are recognized are defined;***
	PE-06(02)_ODP[03]	***automated mechanisms used to recognize classes or types of intrusions and initiate response actions (defined in PE-06(02)_ODP) are defined;***
	PE-06(02)[01]	***<PE-06(02)_ODP[01] classes or types of intrusions>*** are recognized;

PE-06(02)	MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION AND RESPONSES	
	PE-06(02)[02]	***<PE-06(02)_ODP[02] response actions>*** are initiated using ***<PE-06(02)_ODP[03] automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-06(02)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access monitoring; system design documentation; system configuration settings and associated documentation; system audit records; list of response actions to be initiated when specific classes/types of intrusions are recognized; system security plan; privacy plan; other relevant documents or records].
	PE-06(02)-Interview	[SELECT FROM: Organizational personnel with physical access monitoring responsibilities; organizational personnel with information security and privacy responsibilities].
	PE-06(02)-Test	[SELECT FROM: Organizational processes for monitoring physical access; automated mechanisms supporting and/or implementing physical access monitoring; automated mechanisms supporting and/or implementing recognition of classes/types of intrusions and initiation of a response].

PE-06(03)	MONITORING PHYSICAL ACCESS | VIDEO SURVEILLANCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-06(03)_ODP[01]	***operational areas where video surveillance is to be employed are defined;***
	PE-06(03)_ODP[02]	***frequency at which to review video recordings is defined;***
	PE-06(03)_ODP[03]	***time period for which to retain video recordings is defined;***
	PE-06(03)(a)	video surveillance of ***<PE-06(03)_ODP[01] operational areas>*** is employed;
	PE-06(03)(b)	video recordings are reviewed ***<PE-06(03)_ODP[02] frequency>***;
	PE-06(03)(c)	video recordings are retained for ***<PE-06(03)_ODP[03] time period>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-06(03)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access monitoring; video surveillance equipment used to monitor operational areas; video recordings of operational areas where video surveillance is employed; video surveillance equipment logs or records; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	PE-06(03)-Interview	[SELECT FROM: Organizational personnel with physical access monitoring responsibilities; organizational personnel with information security and privacy responsibilities].
	PE-06(03)-Test	[SELECT FROM: Organizational processes for monitoring physical access; mechanisms supporting and/or implementing physical access monitoring; mechanisms supporting and/or implementing video surveillance].

PE-06(04)	MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO SYSTEMS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-06(04)_ODP	***physical spaces containing one or more components of the system are defined;***
	PE-06(04)	physical access to the system is monitored in addition to the physical access monitoring of the facility at ***<PE-06(04)_ODP physical spaces>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-06(04)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing physical access monitoring; physical access control logs or records; physical access control devices; access authorizations; access credentials; list of areas within the facility containing concentrations of system components or system components requiring additional physical access monitoring; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	PE-06(04)-Interview	[SELECT FROM: Organizational personnel with physical access monitoring responsibilities; organizational personnel with information security and privacy responsibilities].
	PE-06(04)-Test	[SELECT FROM: Organizational processes for monitoring physical access to the system; mechanisms supporting and/or implementing physical access monitoring for facility areas containing system components].

PE-07	VISITOR CONTROL
	[WITHDRAWN: Incorporated into PE-02, PE-03.]

PE-08	VISITOR ACCESS RECORDS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-08_ODP[01]	***time period for which to maintain visitor access records for the facility where the system resides is defined;***
	PE-08_ODP[02]	***the frequency at which to review visitor access records is defined;***
	PE-08_ODP[03]	***personnel to whom visitor access records anomalies are reported to is/are defined;***
	PE-08a.	visitor access records for the facility where the system resides are maintained for ***<PE-08_ODP[01] time period>***;
	PE-08b.	visitor access records are reviewed ***<PE-08_ODP[02] frequency>***;
	PE-08c.	visitor access records anomalies are reported to ***<PE-08_ODP[03] personnel>***.

PE-08	VISITOR ACCESS RECORDS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-08-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing visitor access records; visitor access control logs or records; visitor access record or log reviews; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	PE-08-Interview	[SELECT FROM: Organizational personnel with visitor access record responsibilities; organizational personnel with information security and privacy responsibilities].
	PE-08-Test	[SELECT FROM: Organizational processes for maintaining and reviewing visitor access records; mechanisms supporting and/or implementing the maintenance and review of visitor access records].

PE-08(01)	VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE AND REVIEW	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-08(01)_ODP[01]	***automated mechanisms used to maintain visitor access records are defined;***
	PE-08(01)_ODP[02]	***automated mechanisms used to review visitor access records are defined;***
	PE-08(01)[01]	visitor access records are maintained using ***<PE-08(01)_ODP[01] automated mechanisms>***;
	PE-08(01)[02]	visitor access records are reviewed using ***<PE-08(01)_ODP[02] automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-08(01)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing visitor access records; automated mechanisms supporting management of visitor access records; visitor access control logs or records; system security plan; privacy plan; other relevant documents or records].
	PE-08(01)-Interview	[SELECT FROM: Organizational personnel with visitor access record responsibilities; organizational personnel with information security and privacy responsibilities].
	PE-08(01)-Test	[SELECT FROM: Organizational processes for maintaining and reviewing visitor access records; automated mechanisms supporting and/or implementing the maintenance and review of visitor access records].

PE-08(02)	VISITOR ACCESS RECORDS | PHYSICAL ACCESS RECORDS
	[WITHDRAWN: Incorporated into PE-02.]

PE-08(03)	VISITOR ACCESS RECORDS | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-08(03)_ODP	***elements identified in the privacy risk assessment to limit personally identifiable information contained in visitor access logs are defined;***
	PE-08(03)	personally identifiable information contained in visitor access records is limited to ***<PE-08(03)_ODP elements>*** identified in the privacy risk assessment.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-08(03)-Examine	[SELECT FROM: Physical and environmental protection policy; personally identifiable information processing policy; privacy risk assessment documentation; privacy impact assessment; visitor access records; personally identifiable information inventory; system security plan; privacy plan; other relevant documents or records].
	PE-08(03)-Interview	[SELECT FROM: Organizational personnel with visitor access records responsibilities; organizational personnel with information security and privacy responsibilities].
	PE-08(03)-Test	[SELECT FROM: Organizational processes for maintaining and reviewing visitor access records].

PE-09	POWER EQUIPMENT AND CABLING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-09[01]	power equipment for the system is protected from damage and destruction;
	PE-09[02]	power cabling for the system is protected from damage and destruction.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-09-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing power equipment/cabling protection; facilities housing power equipment/cabling; system security plan; other relevant documents or records].
	PE-09-Interview	[SELECT FROM: Organizational personnel with the responsibility to protect power equipment/cabling; organizational personnel with information security responsibilities].
	PE-09-Test	[SELECT FROM: Mechanisms supporting and/or implementing the protection of power equipment/cabling].

PE-09(01)	POWER EQUIPMENT AND CABLING | REDUNDANT CABLING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-09(01)_ODP	***distance by which redundant power cabling paths are to be physically separated is defined;***

PE-09(01)	POWER EQUIPMENT AND CABLING | REDUNDANT CABLING	
	PE-09(01)	redundant power cabling paths that are physically separated by ***<PE-09(01)_ODP distance>*** are employed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-09(01)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing power equipment/cabling protection; facilities housing power equipment/cabling; system security plan; other relevant documents or records].
	PE-09(01)-Interview	[SELECT FROM: Organizational personnel with the responsibility to protect power equipment/cabling; organizational personnel with information security responsibilities].
	PE-09(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the protection of power equipment/cabling].

PE-09(02)	POWER EQUIPMENT AND CABLING | AUTOMATIC VOLTAGE CONTROLS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-09(02)_ODP	***the critical system components that require automatic voltage controls are defined;***
	PE-09(02)	automatic voltage controls for ***<PE-09(02)_ODP critical system components>*** are employed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-09(02)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing voltage control; security plan; list of critical system components requiring automatic voltage controls; automatic voltage control mechanisms and associated configurations; system security plan; other relevant documents or records].
	PE-09(02)-Interview	[SELECT FROM: Organizational personnel with responsibilities for environmental protection of system components; organizational personnel with information security responsibilities].
	PE-09(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing automatic voltage controls].

PE-10	EMERGENCY SHUTOFF	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-10_ODP[01]	***system or individual system components that require the capability to shut off power in emergency situations is/are defined;***
	PE-10_ODP[02]	***location of emergency shutoff switches or devices by system or system component is defined;***
	PE-10a.	the capability to shut off power to ***<PE-10_ODP[01] system or individual system components>*** in emergency situations is provided;

PE-10	EMERGENCY SHUTOFF	
	PE-10b.	emergency shutoff switches or devices are placed in ***<PE-10_ODP[02] location>*** to facilitate access for authorized personnel;
	PE-10c.	the emergency power shutoff capability is protected from unauthorized activation.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-10-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing power source emergency shutoff; emergency shutoff controls or switches; locations housing emergency shutoff switches and devices; security safeguards protecting the emergency power shutoff capability from unauthorized activation; system security plan; other relevant documents or records].
	PE-10-Interview	[SELECT FROM: Organizational personnel with the responsibility for the emergency power shutoff capability (both implementing and using the capability); organizational personnel with information security responsibilities].
	PE-10-Test	[SELECT FROM: Mechanisms supporting and/or implementing emergency power shutoff].

PE-10(01)	EMERGENCY SHUTOFF | ACCIDENTAL AND UNAUTHORIZED ACTIVATION	
	[WITHDRAWN: Incorporated into PE-10.]	

PE-11	EMERGENCY POWER	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-11_ODP	***one of the following PARAMETER VALUES is selected: {an orderly shutdown of the system; transition of the system to long-term alternate power};***
	PE-11	an uninterruptible power supply is provided to facilitate ***<PE-11_ODP SELECTED PARAMETER VALUE>*** in the event of a primary power source loss.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-11-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply; uninterruptible power supply documentation; uninterruptible power supply test records; system security plan; other relevant documents or records].
	PE-11-Interview	[SELECT FROM: Organizational personnel with the responsibility for emergency power and/or planning; organizational personnel with information security responsibilities].
	PE-11-Test	[SELECT FROM: Mechanisms supporting and/or implementing an uninterruptible power supply; the uninterruptable power supply].

PE-11(01)	EMERGENCY POWER | ALTERNATE POWER SUPPLY — MINIMAL OPERATIONAL CAPABILITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-11(01)_ODP	***one of the following PARAMETER VALUES is selected: {manually; automatically};***
	PE-11(01)[01]	an alternate power supply provided for the system is activated ***<PE-11(01)_ODP SELECTED PARAMETER VALUE>***;
	PE-11(01)[02]	the alternate power supply provided for the system can maintain minimally required operational capability in the event of an extended loss of the primary power source.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-11(01)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing emergency power; alternate power supply; alternate power supply documentation; alternate power supply test records; system security plan; other relevant documents or records].
	PE-11(01)-Interview	[SELECT FROM: Organizational personnel with the responsibility for emergency power and/or planning; organizational personnel with information security responsibilities].
	PE-11(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing an alternate power supply; the alternate power supply].

PE-11(02)	EMERGENCY POWER | ALTERNATE POWER SUPPLY — SELF-CONTAINED	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-11(02)_ODP[01]	***one of the following PARAMETER VALUES is selected: {manually; automatically};***
	PE-11(02)_ODP[02]	***one of the following PARAMETER VALUES is selected: {minimally required operational capability; full operational capability};***
	PE-11(02)	an alternate power supply provided for the system is activated ***<PE-11(02)_ODP[01] SELECTED PARAMETER VALUE>***;
	PE-11(02)(a)	the alternate power supply provided for the system is self-contained;
	PE-11(02)(b)	the alternate power supply provided for the system is not reliant on external power generation;
	PE-11(02)(c)	the alternate power supply provided for the system is capable of maintaining ***<PE-11(02)_ODP[02] SELECTED PARAMETER VALUE>*** in the event of an extended loss of the primary power source.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-11(02)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing emergency power; alternate power supply; alternate power supply documentation; alternate power supply test records; system security plan; other relevant documents or records].

PE-11(02)	EMERGENCY POWER | ALTERNATE POWER SUPPLY — SELF-CONTAINED	
	PE-11(02)-Interview	[SELECT FROM: Organizational personnel with the responsibility for emergency power and/or planning; organizational personnel with information security responsibilities].
	PE-11(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing an alternate power supply; the alternate power supply].

PE-12	EMERGENCY LIGHTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-12[01]	automatic emergency lighting that activates in the event of a power outage or disruption is employed for the system;
	PE-12[02]	automatic emergency lighting that activates in the event of a power outage or disruption is maintained for the system;
	PE-12[03]	automatic emergency lighting for the system covers emergency exits within the facility;
	PE-12[04]	automatic emergency lighting for the system covers evacuation routes within the facility.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-12-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; system security plan; other relevant documents or records].
	PE-12-Interview	[SELECT FROM: Organizational personnel with the responsibility for emergency lighting and/or planning; organizational personnel with information security responsibilities].
	PE-12-Test	[SELECT FROM: Mechanisms supporting and/or implementing an emergency lighting capability].

PE-12(01)	EMERGENCY LIGHTING | ESSENTIAL MISSION AND BUSINESS FUNCTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-12(01)	emergency lighting is provided for all areas within the facility supporting essential mission and business functions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-12(01)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing emergency lighting; emergency lighting documentation; emergency lighting test records; emergency exits and evacuation routes; areas/locations within facility supporting essential missions and business functions; system security plan; other relevant documents or records].

PE-12(01)	EMERGENCY LIGHTING | ESSENTIAL MISSION AND BUSINESS FUNCTIONS	
	PE-12(01)-Interview	[SELECT FROM: Organizational personnel with the responsibility for emergency lighting and/or planning; organizational personnel with information security responsibilities].
	PE-12(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the emergency lighting capability].

PE-13	FIRE PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-13[01]	fire detection systems are employed;
	PE-13[02]	employed fire detection systems are supported by an independent energy source;
	PE-13[03]	employed fire detection systems are maintained;
	PE-13[04]	fire suppression systems are employed;
	PE-13[05]	employed fire suppression systems are supported by an independent energy source;
	PE-13[06]	employed fire suppression systems are maintained.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-13-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; test records of fire suppression and detection devices/systems; system security plan; other relevant documents or records].
	PE-13-Interview	[SELECT FROM: Organizational personnel with responsibilities for fire detection and suppression devices/systems; organizational personnel with information security responsibilities].
	PE-13-Test	[SELECT FROM: Mechanisms supporting and/or implementing fire suppression/ detection devices/systems].

PE-13(01)	FIRE PROTECTION | DETECTION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-13(01)_ODP[01]	***personnel or roles to be notified in the event of a fire is/are defined;***
	PE-13(01)_ODP[02]	***emergency responders to be notified in the event of a fire are defined;***
	PE-13(01)[01]	fire detection systems that activate automatically are employed in the event of a fire;
	PE-13(01)[02]	fire detection systems that notify ***<PE-13(01)_ODP[01] personnel or roles>*** automatically are employed in the event of a fire;

PE-13(01)	FIRE PROTECTION | DETECTION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION	
	PE-13(01)[03]	fire detection systems that notify ***<PE-13(01)_ODP[02] emergency responders>*** automatically are employed in the event of a fire.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-13(01)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing fire protection; facility housing the information system; alarm service-level agreements; test records of fire suppression and detection devices/systems; fire suppression and detection devices/systems documentation; alerts/notifications of fire events; system security plan; other relevant documents or records].
	PE-13(01)-Interview	[SELECT FROM: Organizational personnel with responsibilities for fire detection and suppression devices/systems; organizational personnel with responsibilities for notifying appropriate personnel, roles, and emergency responders of fires; organizational personnel with information security responsibilities].
	PE-13(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing fire detection devices/systems; activation of fire detection devices/systems (simulated); automated notifications].

PE-13(02)	FIRE PROTECTION | SUPPRESSION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-13(02)_ODP[01]	***personnel or roles to be notified in the event of a fire is/are defined;***
	PE-13(02)_ODP[02]	***emergency responders to be notified in the event of a fire are defined;***
	PE-13(02)(a)[01]	fire suppression systems that activate automatically are employed;
	PE-13(02)(a)[02]	fire suppression systems that notify ***<PE-13(02)_ODP[01] personnel or roles>*** automatically are employed;
	PE-13(02)(a)[03]	fire suppression systems that notify ***<PE-13(02)_ODP[02] emergency responders>*** automatically are employed;
	PE-13(02)(b)	an automatic fire suppression capability is employed when the facility is not staffed on a continuous basis.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-13(02)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing fire protection; fire suppression and detection devices/systems documentation; facility housing the system; alarm service-level agreements; test records of fire suppression and detection devices/systems; system security plan; other relevant documents or records].
	PE-13(02)-Interview	[SELECT FROM: Organizational personnel with responsibilities for fire detection and suppression devices/systems; organizational personnel with responsibilities for providing automatic notifications of any activation of fire suppression devices/systems to appropriate personnel, roles, and emergency responders; organizational personnel with information security responsibilities].

PE-13(02)	FIRE PROTECTION | SUPPRESSION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION	
	PE-13(02)-Test	[SELECT FROM: Automated mechanisms supporting and/or implementing fire suppression devices/systems; activation of fire suppression devices/systems (simulated); automated notifications].

PE-13(03)	FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION
	[WITHDRAWN: Incorporated into PE-13(02).]

PE-13(04)	FIRE PROTECTION | INSPECTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-13(04)_ODP[01]	***the frequency for conducting fire protection inspections on the facility is defined;***
	PE-13(04)_ODP[02]	***a time period for resolving deficiencies identified by fire protection inspections is defined;***
	PE-13(04)[01]	the facility undergoes fire protection inspections ***<PE-13(04)_ODP[01] frequency>*** by authorized and qualified inspectors;
	PE-13(04)[02]	the identified deficiencies from fire protection inspections are resolved within ***<PE-13(04)_ODP[02] time period>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-13(04)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing fire protection; facility housing the system; inspection plans; inspection results; inspect reports; test records of fire suppression and detection devices/systems; system security plan; other relevant documents or records].
	PE-13(04)-Interview	[SELECT FROM: Organizational personnel with responsibilities for planning, approving, and executing fire inspections; organizational personnel with information security responsibilities].

PE-14	ENVIRONMENTAL CONTROLS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-14_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {temperature; humidity; pressure; radiation; <PE-14_ODP[02] environmental control>};***
	PE-14_ODP[02]	***environmental control(s) for which to maintain a specified level in the facility where the system resides are defined (if selected);***
	PE-14_ODP[03]	***acceptable levels for environmental controls are defined;***
	PE-14_ODP[04]	***frequency at which to monitor environmental control levels is defined;***

PE-14	ENVIRONMENTAL CONTROLS	
	PE-14a.	***<PE-14_ODP[01] SELECTED PARAMETER VALUE(S)>*** levels are maintained at ***<PE-14_ODP[03] acceptable levels>*** within the facility where the system resides;
	PE-14b.	environmental control levels are monitored ***<PE-14_ODP[04] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-14-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing temperature and humidity control; temperature and humidity controls; facility housing the system; temperature and humidity controls documentation; temperature and humidity records; system security plan; other relevant documents or records].
	PE-14-Interview	[SELECT FROM: Organizational personnel with responsibilities for system environmental controls; organizational personnel with information security responsibilities].
	PE-14-Test	[SELECT FROM: Mechanisms supporting and/or implementing the maintenance and monitoring of temperature and humidity levels].

PE-14(01)	ENVIRONMENTAL CONTROLS | AUTOMATIC CONTROLS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-14(01)_ODP	***automatic environmental controls to prevent fluctuations that are potentially harmful to the system are defined;***
	PE-14(01)	***<PE-14(01)_ODP automatic environmental controls>*** are employed in the facility to prevent fluctuations that are potentially harmful to the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-14(01)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing temperature and humidity controls; facility housing the system; automated mechanisms for temperature and humidity; temperature and humidity controls; temperature and humidity documentation; system security plan; other relevant documents or records].
	PE-14(01)-Interview	[SELECT FROM: Organizational personnel with responsibilities for system environmental controls; organizational personnel with information security responsibilities].
	PE-14(01)-Test	[SELECT FROM: Automated mechanisms supporting and/or implementing temperature and humidity levels].

PE-14(02)	ENVIRONMENTAL CONTROLS | MONITORING WITH ALARMS AND NOTIFICATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-14(02)_ODP	***personnel or roles to be notified by environmental control monitoring when environmental changes are potentially harmful to personnel or equipment is/are defined;***

PE-14(02)	ENVIRONMENTAL CONTROLS | MONITORING WITH ALARMS AND NOTIFICATIONS	
	PE-14(02)[01]	environmental control monitoring is employed;
	PE-14(02)[02]	the environmental control monitoring capability provides an alarm or notification to ***<PE-14(02)_ODP personnel or roles>*** when changes are potentially harmful to personnel or equipment.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-14(02)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing temperature and humidity monitoring; facility housing the system; logs or records of temperature and humidity monitoring; records of changes to temperature and humidity levels that generate alarms or notifications; system security plan; other relevant documents or records].
	PE-14(02)-Interview	[SELECT FROM: Organizational personnel with responsibilities for system environmental controls; organizational personnel with information security responsibilities].
	PE-14(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing temperature and humidity monitoring].

PE-15	WATER DAMAGE PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-15[01]	the system is protected from damage resulting from water leakage by providing master shutoff or isolation valves;
	PE-15[02]	the master shutoff or isolation valves are accessible;
	PE-15[03]	the master shutoff or isolation valves are working properly;
	PE-15[04]	the master shutoff or isolation valves are known to key personnel.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-15-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing water damage protection; facility housing the system; master shutoff valves; list of key personnel with knowledge of location and activation procedures for master shutoff valves for the plumbing system; master shutoff valve documentation; system security plan; other relevant documents or records].
	PE-15-Interview	[SELECT FROM: Organizational personnel with responsibilities for system environmental controls; organizational personnel with information security responsibilities].
	PE-15-Test	[SELECT FROM: Master water-shutoff valves; organizational process for activating master water shutoff].

PE-15(01)	WATER DAMAGE PROTECTION | AUTOMATION SUPPORT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-15(01)_ODP[01]	***personnel or roles to be alerted when the presence of water is detected near the system is/are defined;***
	PE-15(01)_ODP[02]	***automated mechanisms used to detect the presence of water near the system are defined;***
	PE-15(01)[01]	the presence of water near the system can be detected automatically;
	PE-15(01)[02]	***<PE-15(01)_ODP[01] personnel or roles>*** is/are alerted using ***<PE-15(01)_ODP[02] automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-15(01)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing water damage protection; facility housing the system; automated mechanisms for water shutoff valves; automated mechanisms for detecting the presence of water in the vicinity of the system; alerts/notifications of water detection in system facility; system security plan; other relevant documents or records].
	PE-15(01)-Interview	[SELECT FROM: Organizational personnel with responsibilities for system environmental controls; organizational personnel with information security responsibilities].
	PE-15(01)-Test	[SELECT FROM: Automated mechanisms supporting and/or implementing water detection capabilities and alerts for the system].

PE-16	DELIVERY AND REMOVAL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-16_ODP[01]	***types of system components to be authorized and controlled when entering the facility are defined;***
	PE-16_ODP[02]	***types of system components to be authorized and controlled when exiting the facility are defined;***
	PE-16a.[01]	***<PE-16_ODP[01] types of system components>*** are authorized when entering the facility;
	PE-16a.[02]	***<PE-16_ODP[01] types of system components>*** are controlled when entering the facility;
	PE-16a.[03]	***<PE-16_ODP[02] types of system components>*** are authorized when exiting the facility;
	PE-16a.[04]	***<PE-16_ODP[02] types of system components>*** are controlled when exiting the facility;
	PE-16b.	records of the system components are maintained.

PE-16	DELIVERY AND REMOVAL	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-16-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing the delivery and removal of system components from the facility; facility housing the system; records of items entering and exiting the facility; system security plan; other relevant documents or records].
	PE-16-Interview	[SELECT FROM: Organizational personnel with responsibilities for controlling system components entering and exiting the facility; organizational personnel with information security responsibilities].
	PE-16-Test	[SELECT FROM: Organizational process for authorizing, monitoring, and controlling system-related items entering and exiting the facility; mechanisms supporting and/or implementing, authorizing, monitoring, and controlling system-related items entering and exiting the facility].

PE-17	ALTERNATE WORK SITE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-17_ODP[01]	***alternate work sites allowed for use by employees are defined;***
	PE-17_ODP[02]	***controls to be employed at alternate work sites are defined;***
	PE-17a.	***<PE-17_ODP[01] alternate work sites>*** are determined and documented;
	PE-17b.	***<PE-17_ODP[02] controls>*** are employed at alternate work sites;
	PE-17c.	the effectiveness of controls at alternate work sites is assessed;
	PE-17d.	a means for employees to communicate with information security and privacy personnel in case of incidents is provided.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-17-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; list of security controls required for alternate work sites; assessments of security controls at alternate work sites; system security plan; privacy plan; other relevant documents or records].
	PE-17-Interview	[SELECT FROM: Organizational personnel approving the use of alternate work sites; organizational personnel using alternate work sites; organizational personnel assessing controls at alternate work sites; organizational personnel with information security and privacy responsibilities].
	PE-17-Test	[SELECT FROM: Organizational processes for security and privacy at alternate work sites; mechanisms supporting alternate work sites; security and privacy controls employed at alternate work sites; means of communication between personnel at alternate work sites and security and privacy personnel].

PE-18	LOCATION OF SYSTEM COMPONENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-18_ODP	***physical and environmental hazards that could result in potential damage to system components within the facility are defined;***
	PE-18	system components are positioned within the facility to minimize potential damage from ***<PE-18_ODP physical and environmental hazards>*** and to minimize the opportunity for unauthorized access.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-18-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing the positioning of system components; documentation providing the location and position of system components within the facility; locations housing system components within the facility; list of physical and environmental hazards with the potential to damage system components within the facility; system security plan; other relevant documents or records].
	PE-18-Interview	[SELECT FROM: Organizational personnel with responsibilities for positioning system components; organizational personnel with information security responsibilities].
	PE-18-Test	[SELECT FROM: Organizational processes for positioning system components].

PE-18(01)	LOCATION OF SYSTEM COMPONENTS | FACILITY SITE
	[WITHDRAWN: Moved to PE-23.]

PE-19	INFORMATION LEAKAGE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-19	the system is protected from information leakage due to electromagnetic signal emanations.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-19-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing information leakage due to electromagnetic signal emanations; mechanisms protecting the system against electronic signal emanations; facility housing the system; records from electromagnetic signal emanation tests; system security plan; other relevant documents or records].
	PE-19-Interview	[SELECT FROM: Organizational personnel with responsibilities for system environmental controls; organizational personnel with information security responsibilities].
	PE-19-Test	[SELECT FROM: Mechanisms supporting and/or implementing protection from information leakage due to electromagnetic signal emanations].

PE-19(01)	INFORMATION LEAKAGE | NATIONAL EMISSIONS POLICIES AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-19(01)[01]	system components are protected in accordance with national emissions security policies and procedures based on the security category or classification of the information;
	PE-19(01)[02]	associated data communications are protected in accordance with national emissions security policies and procedures based on the security category or classification of the information;
	PE-19(01)[03]	networks are protected in accordance with national emissions security policies and procedures based on the security category or classification of the information.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-19(01)-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing information leakage that comply with national emissions and TEMPEST policies and procedures; system component design documentation; system configuration settings and associated documentation system security plan; other relevant documents or records].
	PE-19(01)-Interview	[SELECT FROM: Organizational personnel with responsibilities for system environmental controls; organizational personnel with information security responsibilities].
	PE-19(01)-Test	[SELECT FROM: Information system components for compliance with national emissions and TEMPEST policies and procedures].

PE-20	ASSET MONITORING AND TRACKING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-20_ODP[01]	***asset location technologies to be employed to track and monitor the location and movement of assets is defined;***
	PE-20_ODP[02]	***assets whose location and movement are to be tracked and monitored are defined;***
	PE-20_ODP[03]	***controlled areas within which asset location and movement are to be tracked and monitored are defined;***
	PE-20	***<PE-20_ODP[01] asset location technologies>*** are employed to track and monitor the location and movement of ***<PE-20_ODP[02] assets>*** within ***<PE-20_ODP[03] controlled areas>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-20-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing asset monitoring and tracking; documentation showing the use of asset location technologies; system configuration documentation; list of organizational assets requiring tracking and monitoring; asset monitoring and tracking records; system security plan; privacy plan; other relevant documents or records].

PE-20	ASSET MONITORING AND TRACKING	
	PE-20-Interview	[SELECT FROM: Organizational personnel with asset monitoring and tracking responsibilities; legal counsel; organizational personnel with information security and privacy responsibilities].
	PE-20-Test	[SELECT FROM: Organizational processes for tracking and monitoring assets; mechanisms supporting and/or implementing the tracking and monitoring of assets].

PE-21	ELECTROMAGNETIC PULSE PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-21_ODP[01]	***protective measures to be employed against electromagnetic pulse damage are defined;***
	PE-21_ODP[02]	***system and system components requiring protection against electromagnetic pulse damage are defined;***
	PE-21	***<PE-21_ODP[01] protective measures>*** are employed against electromagnetic pulse damage for ***<PE-21_ODP[02] system and system components>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-21-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing protective measures to mitigate EMP risk to systems and components; documentation detailing protective measures to mitigate EMP risk; list of locations where protective measures to mitigate EMP risk are implemented; system security plan; other relevant documents or records].
	PE-21-Interview	[SELECT FROM: Organizational personnel with responsibilities for physical and environmental protection; system developers/integrators; organizational personnel with information security responsibilities].
	PE-21-Test	[SELECT FROM: Mechanisms for mitigating EMP risk].

PE-22	COMPONENT MARKING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-22_ODP	***system hardware components to be marked indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component are defined;***
	PE-22	***<PE-22_ODP system hardware components>*** are marked indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.

PE-22	COMPONENT MARKING	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-22-Examine	[SELECT FROM: Physical and environmental protection policy; procedures addressing component marking; list of component marking security attributes; component inventory; information types and their impact/classification level; system security plan; other relevant documents or records].
	PE-22-Interview	[SELECT FROM: Organizational personnel with component marking responsibilities; organizational personnel with component inventory responsibilities; organizational personnel with information categorization/classification responsibilities; organizational personnel with information security responsibilities].
	PE-22-Test	[SELECT FROM: Organizational processes for component marking; automated mechanisms supporting and/or implementing component marking].

PE-23	FACILITY LOCATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PE-23a.	the location or site of the facility where the system resides is planned considering physical and environmental hazards;
	PE-23b.	for existing facilities, physical and environmental hazards are considered in the organizational risk management strategy.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PE-23-Examine	[SELECT FROM: Physical and environmental protection policy; physical site planning documents; organizational assessment of risk; contingency plan; risk mitigation strategy documentation; system security plan; other relevant documents or records].
	PE-23-Interview	[SELECT FROM: Organizational personnel with site selection responsibilities for the facility housing the system; organizational personnel with risk mitigation responsibilities; organizational personnel with information security responsibilities].
	PE-23-Test	[SELECT FROM: Organizational processes for site planning].

4.12 PLANNING

PL-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-01_ODP[01]	***personnel or roles to whom the planning policy is to be disseminated is/are defined;***
	PL-01_ODP[02]	***personnel or roles to whom the planning procedures are to be disseminated is/are defined;***
	PL-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	PL-01_ODP[04]	***an official to manage the planning policy and procedures is defined;***
	PL-01_ODP[05]	***the frequency with which the current planning policy is reviewed and updated is defined;***
	PL-01_ODP[06]	***events that would require the current planning policy to be reviewed and updated are defined;***
	PL-01_ODP[07]	***the frequency with which the current planning procedures are reviewed and updated is defined;***
	PL-01_ODP[08]	***events that would require procedures to be reviewed and updated are defined;***
	PL-01a.[01]	a planning policy is developed and documented.
	PL-01a.[02]	the planning policy is disseminated to ***<PL-01_ODP[01] personnel or roles>***;
	PL-01a.[03]	planning procedures to facilitate the implementation of the planning policy and associated planning controls are developed and documented;
	PL-01a.[04]	the planning procedures are disseminated to ***<PL-01_ODP[02] personnel or roles>***;
	PL-01a.01(a)[01]	the ***<PL-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** planning policy addresses purpose;
	PL-01a.01(a)[02]	the ***<PL-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** planning policy addresses scope;
	PL-01a.01(a)[03]	the ***<PL-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** planning policy addresses roles;
	PL-01a.01(a)[04]	the ***<PL-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** planning policy addresses responsibilities;
	PL-01a.01(a)[05]	the ***<PL-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** planning policy addresses management commitment;
	PL-01a.01(a)[06]	the ***<PL-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** planning policy addresses coordination among organizational entities;
	PL-01a.01(a)[07]	the ***<PL-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** planning policy addresses compliance;
	PL-01a.01(b)	the ***<PL-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** planning policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines;

PL-01	POLICY AND PROCEDURES	
	PL-01b.	the ***<PL-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the planning policy and procedures;
	PL-01c.01[01]	the current planning policy is reviewed and updated ***<PL-01_ODP[05] frequency>***;
	PL-01c.01[02]	the current planning policy is reviewed and updated following ***<PL-01_ODP[06] events>***;
	PL-01c.02[01]	the current planning procedures are reviewed and updated ***<PL-01_ODP[07] frequency>***;
	PL-01c.02[02]	the current planning procedures are reviewed and updated following ***<PL-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-01-Examine	[SELECT FROM: Planning policy and procedures; system security plan; privacy plan; other relevant documents or records].
	PL-01-Interview	[SELECT FROM: Organizational personnel with planning responsibilities; organizational personnel with information security and privacy responsibilities].

PL-02	SYSTEM SECURITY AND PRIVACY PLANS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-02_ODP[01]	***individuals or groups with whom security and privacy-related activities affecting the system that require planning and coordination is/are assigned;***
	PL-02_ODP[02]	***personnel or roles to receive distributed copies of the system security and privacy plans is/are assigned;***
	PL-02_ODP[03]	***frequency to review system security and privacy plans is defined;***
	PL-02a.01[01]	a security plan for the system is developed that is consistent with the organization's enterprise architecture;
	PL-02a.01[02]	a privacy plan for the system is developed that is consistent with the organization's enterprise architecture;
	PL-02a.02[01]	a security plan for the system is developed that explicitly defines the constituent system components;
	PL-02a.02[02]	a privacy plan for the system is developed that explicitly defines the constituent system components;
	PL-02a.03[01]	a security plan for the system is developed that describes the operational context of the system in terms of mission and business processes;
	PL-02a.03[02]	a privacy plan for the system is developed that describes the operational context of the system in terms of mission and business processes;
	PL-02a.04[01]	a security plan for the system is developed that identifies the individuals that fulfill system roles and responsibilities;
	PL-02a.04[02]	a privacy plan for the system is developed that identifies the individuals that fulfill system roles and responsibilities;

PL-02	SYSTEM SECURITY AND PRIVACY PLANS	
	PL-02a.05[01]	a security plan for the system is developed that identifies the information types processed, stored, and transmitted by the system;
	PL-02a.05[02]	a privacy plan for the system is developed that identifies the information types processed, stored, and transmitted by the system;
	PL-02a.06[01]	a security plan for the system is developed that provides the security categorization of the system, including supporting rationale;
	PL-02a.06[02]	a privacy plan for the system is developed that provides the security categorization of the system, including supporting rationale;
	PL-02a.07[01]	a security plan for the system is developed that describes any specific threats to the system that are of concern to the organization;
	PL-02a.07[02]	a privacy plan for the system is developed that describes any specific threats to the system that are of concern to the organization;
	PL-02a.08[01]	a security plan for the system is developed that provides the results of a privacy risk assessment for systems processing personally identifiable information;
	PL-02a.08[02]	a privacy plan for the system is developed that provides the results of a privacy risk assessment for systems processing personally identifiable information;
	PL-02a.09[01]	a security plan for the system is developed that describes the operational environment for the system and any dependencies on or connections to other systems or system components;
	PL-02a.09[02]	a privacy plan for the system is developed that describes the operational environment for the system and any dependencies on or connections to other systems or system components;
	PL-02a.10[01]	a security plan for the system is developed that provides an overview of the security requirements for the system;
	PL-02a.10[02]	a privacy plan for the system is developed that provides an overview of the privacy requirements for the system;
	PL-02a.11[01]	a security plan for the system is developed that identifies any relevant control baselines or overlays, if applicable;
	PL-02a.11[02]	a privacy plan for the system is developed that identifies any relevant control baselines or overlays, if applicable;
	PL-02a.12[01]	a security plan for the system is developed that describes the controls in place or planned for meeting the security requirements, including rationale for any tailoring decisions;
	PL-02a.12[02]	a privacy plan for the system is developed that describes the controls in place or planned for meeting the privacy requirements, including rationale for any tailoring decisions;
	PL-02a.13[01]	a security plan for the system is developed that includes risk determinations for security architecture and design decisions;
	PL-02a.13[02]	a privacy plan for the system is developed that includes risk determinations for privacy architecture and design decisions;
	PL-02a.14[01]	a security plan for the system is developed that includes security-related activities affecting the system that require planning and coordination with ***<PL-02_ODP[01] individuals or groups>***;

PL-02	SYSTEM SECURITY AND PRIVACY PLANS	
	PL-02a.14[02]	a privacy plan for the system is developed that includes privacy-related activities affecting the system that require planning and coordination with ***<PL-02_ODP[01] individuals or groups>***;
	PL-02a.15[01]	a security plan for the system is developed that is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
	PL-02a.15[02]	a privacy plan for the system is developed that is reviewed and approved by the authorizing official or designated representative prior to plan implementation.
	PL-02b.[01]	copies of the plans are distributed to ***<PL-02_ODP[02] personnel or roles>***;
	PL-02b.[02]	subsequent changes to the plans are communicated to ***<PL-02_ODP[02] personnel or roles>***;
	PL-02c.	plans are reviewed ***<PL-02_ODP[03] frequency>***;
	PL-02d.[01]	plans are updated to address changes to the system and environment of operations;
	PL-02d.[02]	plans are updated to address problems identified during the plan implementation;
	PL-02d.[03]	plans are updated to address problems identified during control assessments;
	PL-02e.[01]	plans are protected from unauthorized disclosure;
	PL-02e.[02]	plans are protected from unauthorized modification.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-02-Examine	[SELECT FROM: Security and privacy planning policy; procedures addressing system security and privacy plan development and implementation; procedures addressing security and privacy plan reviews and updates; enterprise architecture documentation; system security plan; privacy plan; records of system security and privacy plan reviews and updates; security and privacy architecture and design documentation; risk assessments; risk assessment results; control assessment documentation; other relevant documents or records].
	PL-02-Interview	[SELECT FROM: Organizational personnel with system security and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities].
	PL-02-Test	[SELECT FROM: Organizational processes for system security and privacy plan development, review, update, and approval; mechanisms supporting the system security and privacy plan].

PL-02(01)	SYSTEM SECURITY AND PRIVACY PLANS | CONCEPT OF OPERATIONS
	[WITHDRAWN: Incorporated into PL-07.]

PL-02(02)	SYSTEM SECURITY AND PRIVACY PLANS | FUNCTIONAL ARCHITECTURE
	[WITHDRAWN: Incorporated into PL-08.]

PL-02(03)	SYSTEM SECURITY AND PRIVACY PLANS | PLAN AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES
	[WITHDRAWN: Incorporated into PL-02.]

PL-03	SYSTEM SECURITY PLAN UPDATE
	[WITHDRAWN: Incorporated into PL-02.]

PL-04	RULES OF BEHAVIOR	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-04_ODP[01]	***frequency for reviewing and updating the rules of behavior is defined;***
	PL-04_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {<PL-04_ODP[03] frequency>; when the rules are revised or updated};***
	PL-04_ODP[03]	***frequency for individuals to read and re-acknowledge the rules of behavior is defined (if selected);***
	PL-04a.[01]	rules that describe responsibilities and expected behavior for information and system usage, security, and privacy are established for individuals requiring access to the system;
	PL-04a.[02]	rules that describe responsibilities and expected behavior for information and system usage, security, and privacy are provided to individuals requiring access to the system;
	PL-04b.	before authorizing access to information and the system, a documented acknowledgement from such individuals indicating that they have read, understand, and agree to abide by the rules of behavior is received;
	PL-04c.	rules of behavior are reviewed and updated ***<PL-04_ODP[01] frequency>***;
	PL-04d.	individuals who have acknowledged a previous version of the rules of behavior are required to read and reacknowledge ***<PL-04_ODP[02] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-04-Examine	[SELECT FROM: Security and privacy planning policy; procedures addressing rules of behavior for system users; rules of behavior; signed acknowledgements; records for rules of behavior reviews and updates; other relevant documents or records].
	PL-04-Interview	[SELECT FROM: Organizational personnel with responsibility for establishing, reviewing, and updating rules of behavior; organizational personnel with responsibility for literacy training and awareness and role-based training; organizational personnel who are authorized users of the system and have signed and resigned rules of behavior; organizational personnel with information security and privacy responsibilities].
	PL-04-Test	[SELECT FROM: Organizational processes for establishing, reviewing, disseminating, and updating rules of behavior; mechanisms supporting and/or implementing the establishment, review, dissemination, and update of rules of behavior].

PL-04(01)	RULES OF BEHAVIOR | SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-04(01)(a)	the rules of behavior include restrictions on the use of social media, social networking sites, and external sites/applications;
	PL-04(01)(b)	the rules of behavior include restrictions on posting organizational information on public websites;
	PL-04(01)(c)	the rules of behavior include restrictions on the use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-04(01)-Examine	[SELECT FROM: Security and privacy planning policy; procedures addressing rules of behavior for system users; rules of behavior; training policy; other relevant documents or records].
	PL-04(01)-Interview	[SELECT FROM: Organizational personnel with responsibility for establishing, reviewing, and updating rules of behavior; organizational personnel with responsibility for literacy training and awareness and role-based training; organizational personnel who are authorized users of the system and have signed rules of behavior; organizational personnel with information security and privacy responsibilities].
	PL-04(01)-Test	[SELECT FROM: Organizational processes for establishing rules of behavior; mechanisms supporting and/or implementing the establishment of rules of behavior].

PL-05	PRIVACY IMPACT ASSESSMENT
	[WITHDRAWN: Incorporated into RA-08.]

PL-06	SECURITY-RELATED ACTIVITY PLANNING
	[WITHDRAWN: Incorporated into PL-02.]

PL-07	CONCEPT OF OPERATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-07_ODP	***frequency for review and update of the Concept of Operations (CONOPS) is defined;***
	PL-07a.	a CONOPS for the system describing how the organization intends to operate the system from the perspective of information security and privacy is developed;
	PL-07b.	the CONOPS is reviewed and updated ***<PL-07_ODP frequency>***.

PL-07	CONCEPT OF OPERATIONS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-07-Examine	[SELECT FROM: Security and privacy planning policy; procedures addressing security and privacy CONOPS development; procedures addressing security and privacy CONOPS reviews and updates; security and privacy CONOPS for the system; system security plan; privacy plan; records of security and privacy CONOPS reviews and updates; other relevant documents or records].
	PL-07-Interview	[SELECT FROM: Organizational personnel with security and privacy planning and plan implementation responsibilities; organizational personnel with information security and privacy responsibilities].
	PL-07-Test	[SELECT FROM: Organizational processes for developing, reviewing, and updating the security CONOPS; mechanisms supporting and/or implementing the development, review, and update of the security CONOPS].

PL-08	SECURITY AND PRIVACY ARCHITECTURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-08_ODP	***frequency for review and update to reflect changes in the enterprise architecture;***
	PL-08a.01	a security architecture for the system describes the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
	PL-08a.02	a privacy architecture describes the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
	PL-08a.03[01]	a security architecture for the system describes how the architecture is integrated into and supports the enterprise architecture;
	PL-08a.03[02]	a privacy architecture for the system describes how the architecture is integrated into and supports the enterprise architecture;
	PL-08a.04[01]	a security architecture for the system describes any assumptions about and dependencies on external systems and services;
	PL-08a.04[02]	a privacy architecture for the system describes any assumptions about and dependencies on external systems and services;
	PL-08b.	changes in the enterprise architecture are reviewed and updated ***<PL-08_ODP frequency>*** to reflect changes in the enterprise architecture;
	PL-08c.[01]	planned architecture changes are reflected in the security plan;
	PL-08c.[02]	planned architecture changes are reflected in the privacy plan;
	PL-08c.[03]	planned architecture changes are reflected in the Concept of Operations (CONOPS);
	PL-08c.[04]	planned architecture changes are reflected in criticality analysis;
	PL-08c.[05]	planned architecture changes are reflected in organizational procedures;
	PL-08c.[06]	planned architecture changes are reflected in procurements and acquisitions.

PL-08	SECURITY AND PRIVACY ARCHITECTURES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-08-Examine	[SELECT FROM: Security and privacy planning policy; procedures addressing information security and privacy architecture development; procedures addressing information security and privacy architecture reviews and updates; enterprise architecture documentation; information security and privacy architecture documentation; system security plan; privacy plan; security and privacy CONOPS for the system; records of information security and privacy architecture reviews and updates; other relevant documents or records].
	PL-08-Interview	[SELECT FROM: Organizational personnel with security and privacy planning and plan implementation responsibilities; organizational personnel with information security and privacy architecture development responsibilities; organizational personnel with information security and privacy responsibilities].
	PL-08-Test	[SELECT FROM: Organizational processes for developing, reviewing, and updating the information security and privacy architecture; mechanisms supporting and/or implementing the development, review, and update of the information security and privacy architecture].

PL-08(01)	SECURITY AND PRIVACY ARCHITECTURES | DEFENSE IN DEPTH	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-08(01)_ODP[01]	***controls to be allocated are defined;***
	PL-08(01)_ODP[02]	***locations and architectural layers are defined;***
	PL-08(01)(a)[01]	the security architecture for the system is designed using a defense-in-depth approach that allocates ***<PL-08(01)_ODP[01] controls>*** to ***<PL-08(01)_ODP[02] locations and architectural layers>***;
	PL-08(01)(a)[02]	the privacy architecture for the system is designed using a defense-in-depth approach that allocates ***<PL-08(01)_ODP[01] controls>*** to ***<PL-08(01)_ODP[02] locations and architectural layers>***;
	PL-08(01)(b)[01]	the security architecture for the system is designed using a defense-in-depth approach that ensures the allocated controls operate in a coordinated and mutually reinforcing manner;
	PL-08(01)(b)[02]	the privacy architecture for the system is designed using a defense-in-depth approach that ensures the allocated controls operate in a coordinated and mutually reinforcing manner.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-08-Examine	[SELECT FROM: Security and privacy planning policy; procedures addressing information security and privacy architecture development; enterprise architecture documentation; information security and privacy architecture documentation; system security plan; privacy plan; security and privacy CONOPS for the system; other relevant documents or records].
	PL-08-Interview	[SELECT FROM: Organizational personnel with security and privacy planning and plan implementation responsibilities; organizational personnel with information security and privacy architecture development responsibilities; organizational personnel with information security and privacy responsibilities].

PL-08(01)	SECURITY AND PRIVACY ARCHITECTURES | DEFENSE IN DEPTH	
	PL-08-Test	[SELECT FROM: Organizational processes for designing the information security and privacy architecture; mechanisms supporting and/or implementing the design of the information security and privacy architecture].

PL-08(02)	SECURITY AND PRIVACY ARCHITECTURES | SUPPLIER DIVERSITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-08(02)_ODP[01]	***controls to be allocated are defined;***
	PL-08(02)_ODP[02]	***locations and architectural layers are defined;***
	PL-08(02)	***<PL-08(02)_ODP[01] controls>*** that are allocated to ***<PL-08(02)_ODP[02] locations and architectural layers>*** are required to be obtained from different suppliers.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-08(02)-Examine	[SELECT FROM: Security and privacy planning policy; procedures addressing information security and privacy architecture development; enterprise architecture documentation; information security and privacy architecture documentation; system security plan; privacy plan; security and privacy CONOPS for the system; IT acquisitions policy; other relevant documents or records].
	PL-08(02)-Interview	[SELECT FROM: Organizational personnel with security and privacy planning and plan implementation responsibilities; organizational personnel with information security and privacy architecture development responsibilities; organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities].
	PL-08(02)-Test	[SELECT FROM: Organizational processes for obtaining information security and privacy safeguards from different suppliers].

PL-09	CENTRAL MANAGEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-09_ODP	***security and privacy controls and related processes to be centrally managed are defined;***
	PL-09	***<PL-09_ODP controls and related processes>*** are centrally managed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-09-Examine	[SELECT FROM: Security and privacy planning policy; procedures addressing security and privacy plan development and implementation; system security plan; privacy plan; other relevant documents or records].
	PL-09-Interview	[SELECT FROM: Organizational personnel with security and privacy planning and plan implementation responsibilities; organizational personnel with responsibilities for planning/implementing central management of controls and related processes; organizational personnel with information security and privacy responsibilities].

PL-09	CENTRAL MANAGEMENT	
	PL-09-Test	[SELECT FROM: Organizational processes for the central management of controls and related processes; mechanisms supporting and/or implementing central management of controls and related processes].

PL-10	BASELINE SELECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-10	a control baseline for the system is selected.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-10-Examine	[SELECT FROM: Security and privacy planning policy; procedures addressing system security and privacy plan development and implementation; procedures addressing system security and privacy plan reviews and updates; system design documentation; system architecture and configuration documentation; system categorization decision; information types stored, transmitted, and processed by the system; system element/component information; stakeholder needs analysis; list of security and privacy requirements allocated to the system, system elements, and environment of operation; list of contractual requirements allocated to external providers of the system or system element; business impact analysis or criticality analysis; risk assessments; risk management strategy; organizational security and privacy policy; federal or organization-approved or mandated baselines or overlays; system security plan; privacy plan; other relevant documents or records].
	PL-10-Interview	[SELECT FROM: Organizational personnel with security and privacy planning and plan implementation responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with responsibility for organizational risk management activities].

PL-11	BASELINE TAILORING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PL-11	the selected control baseline is tailored by applying specified tailoring actions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PL-11-Examine	[SELECT FROM: Security and privacy planning policy; procedures addressing system security and privacy plan development and implementation; system design documentation; system categorization decision; information types stored, transmitted, and processed by the system; system element/component information; stakeholder needs analysis; list of security and privacy requirements allocated to the system, system elements, and environment of operation; list of contractual requirements allocated to external providers of the system or system element; business impact analysis or criticality analysis; risk assessments; risk management strategy; organizational security and privacy policy; federal or organization-approved or mandated baselines or overlays; baseline tailoring rationale; system security plan; privacy plan; records of system security and privacy plan reviews and updates; other relevant documents or records].

PL-11	BASELINE TAILORING	
	PL-11-Interview	[SELECT FROM: Organizational personnel with security and privacy planning and plan implementation responsibilities; organizational personnel with information security and privacy responsibilities].

4.13 PROGRAM MANAGEMENT

PM-01	INFORMATION SECURITY PROGRAM PLAN	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-01_ODP[01]	***the frequency at which to review and update the organization-wide information security program plan is defined;***
	PM-01_ODP[02]	***events that trigger the review and update of the organization-wide information security program plan are defined;***
	PM-01a.[01]	an organization-wide information security program plan is developed;
	PM-01a.[02]	the information security program plan is disseminated;
	PM-01a.01[01]	the information security program plan provides an overview of the requirements for the security program;
	PM-01a.01[02]	the information security program plan provides a description of the security program management controls in place or planned for meeting those requirements;
	PM-01a.01[03]	the information security program plan provides a description of the common controls in place or planned for meeting those requirements;
	PM-01a.02[01]	the information security program plan includes the identification and assignment of roles;
	PM-01a.02[02]	the information security program plan includes the identification and assignment of responsibilities;
	PM-01a.02[03]	the information security program plan addresses management commitment;
	PM-01a.02[04]	the information security program plan addresses coordination among organizational entities;
	PM-01a.02[05]	the information security program plan addresses compliance;
	PM-01a.03	the information security program plan reflects the coordination among the organizational entities responsible for information security;
	PM-01a.04	the information security program plan is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;
	PM-01b.[01]	the information security program plan is reviewed and updated ***<PM-01_ODP[01] frequency>***;
	PM-01b.[02]	the information security program plan is reviewed and updated following ***<PM-01_ODP[02] events>***;
	PM-01c.[01]	the information security program plan is protected from unauthorized disclosure;
	PM-01c.[02]	the information security program plan is protected from unauthorized modification.

PM-01	INFORMATION SECURITY PROGRAM PLAN	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-01-Examine	[SELECT FROM: Information security program plan; procedures addressing program plan development and implementation; procedures addressing program plan reviews and updates; procedures addressing coordination of the program plan with relevant entities; procedures for program plan approvals; records of program plan reviews and updates; other relevant documents or records].
	PM-01-Interview	[SELECT FROM: Organizational personnel with information security program planning and plan implementation responsibilities; organizational personnel with information security responsibilities].
	PM-01-Test	[SELECT FROM: Organizational processes for information security program plan development, review, update, and approval; mechanisms supporting and/or implementing the information security program plan].

PM-02	INFORMATION SECURITY PROGRAM LEADERSHIP ROLE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-02[01]	a senior agency information security officer is appointed;
	PM-02[02]	the senior agency information security officer is provided with the mission and resources to coordinate an organization-wide information security program;
	PM-02[03]	the senior agency information security officer is provided with the mission and resources to develop an organization-wide information security program;
	PM-02[04]	the senior agency information security officer is provided with the mission and resources to implement an organization-wide information security program;
	PM-02[05]	the senior agency information security officer is provided with the mission and resources to maintain an organization-wide information security program.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-02-Examine	[SELECT FROM: Information security program plan; procedures addressing program plan development and implementation; procedures addressing program plan reviews and updates; procedures addressing coordination of the program plan with relevant entities; other relevant documents or records].
	PM-02-Interview	[SELECT FROM: Organizational personnel with information security program planning and plan implementation responsibilities; senior information security officer; organizational personnel with information security responsibilities].

PM-03	INFORMATION SECURITY AND PRIVACY RESOURCES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-03a.[01]	the resources needed to implement the information security program are included in capital planning and investment requests, and all exceptions are documented;

PM-03	INFORMATION SECURITY AND PRIVACY RESOURCES	
	PM-03a.[02]	the resources needed to implement the privacy program are included in capital planning and investment requests, and all exceptions are documented;
	PM-03b.[01]	the documentation required for addressing the information security program in capital planning and investment requests is prepared in accordance with applicable laws, executive orders, directives, policies, regulations, standards;
	PM-03b.[02]	the documentation required for addressing the privacy program in capital planning and investment requests is prepared in accordance with applicable laws, executive orders, directives, policies, regulations, standards;
	PM-03c.[01]	information security resources are made available for expenditure as planned;
	PM-03c.[02]	privacy resources are made available for expenditure as planned.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-03-Examine	[SELECT FROM: Information security program plan; Exhibit 300; Exhibit 53; business cases for capital planning and investment; procedures for capital planning and investment; documentation of exceptions to capital planning requirements; other relevant documents or records].
	PM-03-Interview	[SELECT FROM: Organizational personnel with information security program planning responsibilities; organizational personnel with privacy program planning responsibilities; organizational personnel responsible for capital planning and investment; organizational personnel with information security responsibilities; organizational personnel with privacy responsibilities].
	PM-03-Test	[SELECT FROM: Organizational processes for capital planning and investment; organizational processes for business case, Exhibit 300, and Exhibit 53 development; mechanisms supporting the capital planning and investment process].

PM-04	PLAN OF ACTION AND MILESTONES PROCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-04a.01[01]	a process to ensure that plans of action and milestones for the information security program and associated organizational systems are developed;
	PM-04a.01[02]	a process to ensure that plans of action and milestones for the information security program and associated organizational systems are maintained;
	PM-04a.01[03]	a process to ensure that plans of action and milestones for the privacy program and associated organizational systems are developed;
	PM-04a.01[04]	a process to ensure that plans of action and milestones for the privacy program and associated organizational systems are maintained;
	PM-04a.01[05]	a process to ensure that plans of action and milestones for the supply chain risk management program and associated organizational systems are developed;
	PM-04a.01[06]	a process to ensure that plans of action and milestones for the supply chain risk management program and associated organizational systems are maintained;

PM-04	PLAN OF ACTION AND MILESTONES PROCESS	
	PM-04a.02[01]	a process to ensure that plans of action and milestones for the information security program and associated organizational systems document remedial information security risk management actions to adequately respond to risks to organizational operations and assets, individuals, other organizations, and the Nation;
	PM-04a.02[02]	a process to ensure that plans of action and milestones for the privacy program and associated organizational systems document remedial privacy risk management actions to adequately respond to risks to organizational operations and assets, individuals, other organizations, and the Nation;
	PM-04a.02[03]	a process to ensure that plans of action and milestones for the supply chain risk management program and associated organizational systems document remedial supply chain risk management actions to adequately respond to risks to organizational operations and assets, individuals, other organizations, and the Nation;
	PM-04a.03[01]	a process to ensure that plans of action and milestones for the information security risk management programs and associated organizational systems are reported in accordance with established reporting requirements;
	PM-04a.03[02]	a process to ensure that plans of action and milestones for the privacy risk management programs and associated organizational systems are reported in accordance with established reporting requirements;
	PM-04a.03[03]	a process to ensure that plans of action and milestones for the supply chain risk management programs and associated organizational systems are reported in accordance with established reporting requirements;
	PM-04b.[01]	plans of action and milestones are reviewed for consistency with the organizational risk management strategy;
	PM-04b.[02]	plans of action and milestones are reviewed for consistency with organization-wide priorities for risk response actions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-04-Examine	[SELECT FROM: Information security program plan; plans of action and milestones; procedures addressing plans of action and milestones development and maintenance; procedures addressing plans of action and milestones reporting; procedures for reviewing plans of action and milestones for consistency with risk management strategy and risk response priorities; results of risk assessments associated with plans of action and milestones; OMB FISMA reporting requirements; other relevant documents or records].
	PM-04-Interview	[SELECT FROM: Organizational personnel with responsibilities for developing, maintaining, reviewing, and reporting plans of action and milestones; organizational personnel with information security responsibilities].
	PM-04-Test	[SELECT FROM: Organizational processes for plan of action and milestones development, review, maintenance, and reporting; mechanisms supporting plans of action and milestones].

PM-05	SYSTEM INVENTORY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-05_ODP	***the frequency at which to update the inventory of organizational systems is defined;***
	PM-05[01]	an inventory of organizational systems is developed;
	PM-05[02]	the inventory of organizational systems is updated ***<PM-05_ODP frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-05-Examine	[SELECT FROM: Information security program plan; system inventory; procedures addressing system inventory development and maintenance; OMB FISMA reporting guidance; other relevant documents or records].
	PM-05-Interview	[SELECT FROM: Organizational personnel with information security program planning and plan implementation responsibilities; organizational personnel responsible for developing and maintaining the system inventory; organizational personnel with information security responsibilities].
	PM-05-Test	[SELECT FROM: Organizational processes for system inventory development and maintenance; mechanisms supporting the system inventory].

PM-05(01)	SYSTEM INVENTORY | INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-05(01)_ODP	***the frequency at which to update the inventory of systems, applications, and projects that process personally identifiable information is defined;***
	PM-05(01)[01]	an inventory of all systems, applications, and projects that process personally identifiable information is established;
	PM-05(01)[02]	an inventory of all systems, applications, and projects that process personally identifiable information is maintained;
	PM-05(01)[03]	an inventory of all systems, applications, and projects that process personally identifiable information is updated ***<PM-05(01)_ODP frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-05(01)-Examine	[SELECT FROM: Procedures addressing system inventory development, maintenance, and updates; OMB FISMA reporting guidance; privacy program plan; information security program plan; personally identifiable information processing policy; system inventory; personally identifiable information inventory; data mapping documentation; other relevant documents or records].
	PM-05(01)-Interview	[SELECT FROM: Organizational personnel with privacy program planning and plan implementation responsibilities; organizational personnel responsible for developing and maintaining the system inventory; organizational personnel with information security and privacy responsibilities].
	PM-05(01)-Test	[SELECT FROM: Organizational processes for system inventory development, maintenance, and updates; mechanisms supporting the system inventory].

PM-06	MEASURES OF PERFORMANCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-06[01]	information security measures of performance are developed;
	PM-06[02]	information security measures of performance are monitored;
	PM-06[03]	the results of information security measures of performance are reported;
	PM-06[04]	privacy measures of performance are developed;
	PM-06[05]	privacy measures of performance are monitored;
	PM-06[06]	the results of privacy measures of performance are reported.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-06-Examine	[SELECT FROM: Information security program plan; privacy program plan; information security measures of performance; privacy measures of performance; procedures addressing the development, monitoring, and reporting of information security and privacy measures of performance; risk management strategy; other relevant documents or records].
	PM-06-Interview	[SELECT FROM: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for developing, monitoring, and reporting information security and privacy measures of performance; organizational personnel with information security and privacy responsibilities].
	PM-06-Test	[SELECT FROM: Organizational processes for developing, monitoring, and reporting information security and privacy measures of performance; mechanisms supporting the development, monitoring, and reporting of information security and privacy measures of performance].

PM-07	ENTERPRISE ARCHITECTURE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-07[01]	an enterprise architecture is developed with consideration for information security;
	PM-07[02]	an enterprise architecture is maintained with consideration for information security;
	PM-07[03]	an enterprise architecture is developed with consideration for privacy;
	PM-07[04]	an enterprise architecture is maintained with consideration for privacy;
	PM-07[05]	an enterprise architecture is developed with consideration for the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation;
	PM-07[06]	an enterprise architecture is maintained with consideration for the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.

PM-07	ENTERPRISE ARCHITECTURE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-07-Examine	[SELECT FROM: Information security program plan; privacy program plan; enterprise architecture documentation; procedures addressing enterprise architecture development; results of risk assessments of enterprise architecture; other relevant documents or records].
	PM-07-Interview	[SELECT FROM: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for developing enterprise architecture; organizational personnel responsible for risk assessments of enterprise architecture; organizational personnel with information security and privacy responsibilities].
	PM-07-Test	[SELECT FROM: Organizational processes for enterprise architecture development; mechanisms supporting the enterprise architecture and its development].

PM-07(01)	ENTERPRISE ARCHITECTURE | OFFLOADING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-07(01)_ODP	***non-essential functions or services to be offloaded are defined;***
	PM-07(01)	***<PM-07(01)_ODP non-essential functions or services>*** are offloaded to other systems, system components, or an external provider.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-07(01)-Examine	[SELECT FROM: Information security program plan; privacy program plan; enterprise architecture documentation; procedures addressing enterprise architecture development; procedures for identifying and offloading functions or services; results of risk assessments of enterprise architecture; other relevant documents or records].
	PM-07(01)-Interview	[SELECT FROM: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for developing enterprise architecture; organizational personnel responsible for risk assessments of enterprise architecture; organizational personnel with information security and privacy responsibilities].
	PM-07(01)-Test	[SELECT FROM: Organizational processes for enterprise architecture development; mechanisms supporting the enterprise architecture and its development; mechanisms for offloading functions and services].

PM-08	CRITICAL INFRASTRUCTURE PLAN	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-08[01]	information security issues are addressed in the development of a critical infrastructure and key resources protection plan;
	PM-08[02]	information security issues are addressed in the documentation of a critical infrastructure and key resources protection plan;

PM-08	CRITICAL INFRASTRUCTURE PLAN	
	PM-08[03]	information security issues are addressed in the update of a critical infrastructure and key resources protection plan;
	PM-08[04]	privacy issues are addressed in the development of a critical infrastructure and key resources protection plan;
	PM-08[05]	privacy issues are addressed in the documentation of a critical infrastructure and key resources protection plan;
	PM-08[06]	privacy issues are addressed in the update of a critical infrastructure and key resources protection plan.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-08-Examine	[SELECT FROM: Information security program plan; privacy program plan; critical infrastructure and key resources protection plan; procedures addressing the development, documentation, and updating of the critical infrastructure and key resources protection plan; HSPD 7; National Infrastructure Protection Plan; other relevant documents or records].
	PM-08-Interview	[SELECT FROM: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for developing, documenting, and updating the critical infrastructure and key resources protection plan; organizational personnel with information security and privacy responsibilities].
	PM-08-Test	[SELECT FROM: Organizational processes for developing, documenting, and updating the critical infrastructure and key resources protection plan; mechanisms supporting the development, documentation, and updating of the critical infrastructure and key resources protection plan].

PM-09	RISK MANAGEMENT STRATEGY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-09_ODP	***the frequency at which to review and update the risk management strategy is defined;***
	PM-09a.01	a comprehensive strategy is developed to manage security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems;
	PM-09a.02	a comprehensive strategy is developed to manage privacy risk to individuals resulting from the authorized processing of personally identifiable information;
	PM-09b.	the risk management strategy is implemented consistently across the organization;
	PM-09c.	the risk management strategy is reviewed and updated ***<PM-09_ODP frequency>*** or as required to address organizational changes.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-09-Examine	[SELECT FROM: Information security program plan; privacy program plan; risk management strategy; supply chain risk management strategy; procedures addressing the development, implementation, review, and update of the risk management strategy; risk assessment results relevant to the risk management strategy; other relevant documents or records].

PM-09	RISK MANAGEMENT STRATEGY	
	PM-09-Interview	[SELECT FROM: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for the development, implementation, review, and update of the risk management strategy; organizational personnel with information security and privacy responsibilities].
	PM-09-Test	[SELECT FROM: Organizational processes for the development, implementation, review, and update of the risk management strategy; mechanisms supporting the development, implementation, review, and update of the risk management strategy].

PM-10	AUTHORIZATION PROCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-10a.[01]	the security state of organizational systems and the environments in which those systems operate are managed through authorization processes;
	PM-10a.[02]	the privacy state of organizational systems and the environments in which those systems operate are managed through authorization processes;
	PM-10b.	individuals are designated to fulfill specific roles and responsibilities within the organizational risk management process;
	PM-10c.	the authorization processes are integrated into an organization-wide risk management program.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-10-Examine	[SELECT FROM: Information security program plan; privacy program plan; procedures addressing management (i.e., documentation, tracking, and reporting) of the authorization process; assessment, authorization, and monitoring policy; assessment, authorization, and monitoring procedures; system authorization documentation; lists or other documentation about authorization process roles and responsibilities; risk assessment results relevant to the authorization process and the organization-wide risk management program; organizational risk management strategy; other relevant documents or records].
	PM-10-Interview	[SELECT FROM: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for management of the authorization process; organizational personnel with information security and privacy responsibilities].
	PM-10-Test	[SELECT FROM: Organizational processes for authorization; mechanisms supporting the authorization process].

PM-11	MISSION AND BUSINESS PROCESS DEFINITION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-11_ODP	***the frequency at which to review and revise the mission and business processes is defined;***

PM-11	MISSION AND BUSINESS PROCESS DEFINITION	
	PM-11a.[01]	organizational mission and business processes are defined with consideration for information security;
	PM-11a.[02]	organizational mission and business processes are defined with consideration for privacy;
	PM-11a.[03]	organizational mission and business processes are defined with consideration for the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation;
	PM-11b.[01]	information protection needs arising from the defined mission and business processes are determined;
	PM-11b.[02]	personally identifiable information processing needs arising from the defined mission and business processes are determined;
	PM-11c.	the mission and business processes are reviewed and revised ***<PM-11_ODP frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-11-Examine	[SELECT FROM: Information security program plan; privacy program plan; risk management strategy; procedures for determining mission and business protection needs; information security and privacy risk assessment results relevant to the determination of mission and business protection needs; personally identifiable information processing policy; personally identifiable information inventory; other relevant documents or records].
	PM-11-Interview	[SELECT FROM: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for enterprise risk management; organizational personnel responsible for determining information protection needs for mission and business processes; organizational personnel with information security and privacy responsibilities].
	PM-11-Test	[SELECT FROM: Organizational processes for defining mission and business processes and their information protection needs].

PM-12	INSIDER THREAT PROGRAM	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-12	an insider threat program that includes a cross-discipline insider threat incident handling team is implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-12-Interview	[SELECT FROM: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for the insider threat program; members of the cross-discipline insider threat incident handling team; legal counsel; organizational personnel with information security and privacy responsibilities].

PM-12	INSIDER THREAT PROGRAM	
	PM-12-Test	[SELECT FROM: Organizational processes for implementing the insider threat program and the cross-discipline insider threat incident handling team; mechanisms supporting and/or implementing the insider threat program and the cross-discipline insider threat incident handling team].

PM-13	SECURITY AND PRIVACY WORKFORCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-13[01]	a security workforce development and improvement program is established;
	PM-13[02]	a privacy workforce development and improvement program is established.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-13-Examine	[SELECT FROM: Information security program plan; privacy program plan; information security and privacy workforce development and improvement program documentation; procedures for the information security and privacy workforce development and improvement program; information security and privacy role-based training program documentation; other relevant documents or records].
	PM-13-Interview	[SELECT FROM: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for the information security and privacy workforce development and improvement program; organizational personnel with information security and privacy responsibilities].
	PM-13-Test	[SELECT FROM: Organizational processes for implementing the information security and privacy workforce development and improvement program; mechanisms supporting and/or implementing the information security and privacy workforce development and improvement program].

PM-14	TESTING, TRAINING, AND MONITORING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-14a.01[01]	a process is implemented for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational systems are developed;
	PM-14a.01[02]	a process is implemented for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational systems are maintained;
	PM-14a.01[03]	a process is implemented for ensuring that organizational plans for conducting privacy testing, training, and monitoring activities associated with organizational systems are developed;
	PM-14a.01[04]	a process is implemented for ensuring that organizational plans for conducting privacy testing, training, and monitoring activities associated with organizational systems are maintained;

PM-14	TESTING, TRAINING, AND MONITORING	
	PM-14a.02[01]	a process is implemented for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational systems continue to be executed;
	PM-14a.02[02]	a process is implemented for ensuring that organizational plans for conducting privacy testing, training, and monitoring activities associated with organizational systems continue to be executed;
	PM-14b.[01]	testing plans are reviewed for consistency with the organizational risk management strategy;
	PM-14b.[02]	training plans are reviewed for consistency with the organizational risk management strategy;
	PM-14b.[03]	monitoring plans are reviewed for consistency with the organizational risk management strategy;
	PM-14b.[04]	testing plans are reviewed for consistency with organization-wide priorities for risk response actions;
	PM-14b.[05]	training plans are reviewed for consistency with organization-wide priorities for risk response actions;
	PM-14b.[06]	monitoring plans are reviewed for consistency with organization-wide priorities for risk response actions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-14-Examine	[SELECT FROM: Information security program plan; privacy program plan; plans for conducting security and privacy testing, training, and monitoring activities; organizational procedures addressing the development and maintenance of plans for conducting security and privacy testing, training, and monitoring activities; risk management strategy; procedures for the review of plans for conducting security and privacy testing, training, and monitoring activities for consistency with risk management strategy and risk response priorities; results of risk assessments associated with conducting security and privacy testing, training, and monitoring activities; documentation of the timely execution of plans for conducting security and privacy testing, training, and monitoring activities; other relevant documents or records].
	PM-14-Interview	[SELECT FROM: Organizational personnel with responsibilities for developing and maintaining plans for conducting security and privacy testing, training, and monitoring activities; organizational personnel with information security and privacy responsibilities].
	PM-14-Test	[SELECT FROM: Organizational processes for the development and maintenance of plans for conducting security and privacy testing, training, and monitoring activities; mechanisms supporting the development and maintenance of plans for conducting security and privacy testing, training, and monitoring activities].

PM-15	SECURITY AND PRIVACY GROUPS AND ASSOCIATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-15a.[01]	contact is established and institutionalized with selected groups and associations within the security community to facilitate ongoing security education and training for organizational personnel;
	PM-15a.[02]	contact is established and institutionalized with selected groups and associations within the privacy community to facilitate ongoing privacy education and training for organizational personnel;
	PM-15b.[01]	contact is established and institutionalized with selected groups and associations within the security community to maintain currency with recommended security practices, techniques, and technologies;
	PM-15b.[02]	contact is established and institutionalized with selected groups and associations within the privacy community to maintain currency with recommended privacy practices, techniques, and technologies;
	PM-15c.[01]	contact is established and institutionalized with selected groups and associations within the security community to share current security information, including threats, vulnerabilities, and incidents;
	PM-15c.[02]	contact is established and institutionalized with selected groups and associations within the privacy community to share current privacy information, including threats, vulnerabilities, and incidents.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-15-Examine	[SELECT FROM: Information security program plan; privacy program plan; risk management strategy; procedures for establishing and institutionalizing contacts with security and privacy groups and associations; lists or other records of contacts with and/or membership in security and privacy groups and associations; other relevant documents or records].
	PM-15-Interview	[SELECT FROM: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for establishing and institutionalizing contact with security and privacy groups and associations; organizational personnel with information security and privacy responsibilities; personnel from selected groups and associations with which the organization has established and institutionalized contact].
	PM-15-Test	[SELECT FROM: Organizational processes for establishing and institutionalizing contact with security and privacy groups and associations; mechanisms supporting contact with security and privacy groups and associations].

PM-16	THREAT AWARENESS PROGRAM	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-16	a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence is implemented.

PM-16	THREAT AWARENESS PROGRAM	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-16-Examine	[SELECT FROM: Information security program plan; privacy program plan; threat awareness program policy; threat awareness program procedures; risk assessment results relevant to threat awareness; documentation about the cross-organization information-sharing capability; other relevant documents or records].
	PM-16-Interview	[SELECT FROM: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for the threat awareness program; organizational personnel responsible for the cross-organization information-sharing capability; organizational personnel with information security and privacy responsibilities; external personnel with whom threat awareness information is shared by the organization].
	PM-16-Test	[SELECT FROM: Organizational processes for implementing the threat awareness program; organizational processes for implementing the cross-organization information-sharing capability; mechanisms supporting and/or implementing the threat awareness program; mechanisms supporting and/or implementing the cross-organization information-sharing capability].

PM-16(01)	THREAT AWARENESS PROGRAM | AUTOMATED MEANS FOR SHARING THREAT INTELLIGENCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-16(01)	automated mechanisms are employed to maximize the effectiveness of sharing threat intelligence information.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-16(01)-Examine	[SELECT FROM: Information security program plan; privacy program plan; threat awareness program policy; threat awareness program procedures; risk assessment results related to threat awareness; documentation about the cross-organization information-sharing capability; other relevant documents or records].
	PM-16(01)-Interview	[SELECT FROM: Organizational personnel with information security and privacy program planning and plan implementation responsibilities; organizational personnel responsible for the threat awareness program; organizational personnel responsible for the cross-organization information-sharing capability; organizational personnel with information security and privacy responsibilities; external personnel with whom threat awareness information is shared by the organization].
	PM-16(01)-Test	[SELECT FROM: Organizational processes for implementing the threat awareness program; organizational processes for implementing the cross-organization information-sharing capability; automated mechanisms supporting and/or implementing the threat awareness program; automated mechanisms supporting and/or implementing the cross-organization information-sharing capability].

PM-17	PROTECTING CONTROLLED UNCLASSIFIED INFORMATION ON EXTERNAL SYSTEMS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-17_ODP[01]	***the frequency at which to review and update the policy is defined;***
	PM-17_ODP[02]	***the frequency at which to review and update the procedures is defined;***
	PM-17a.[01]	policy is established to ensure that requirements for the protection of controlled unclassified information that is processed, stored, or transmitted on external systems are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards;
	PM-17a.[02]	procedures are established to ensure that requirements for the protection of controlled unclassified information that is processed, stored, or transmitted on external systems are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards;
	PM-17b.[01]	policy is reviewed and updated ***<PM-17_ODP[01] frequency>***;
	PM-17b.[02]	procedures are reviewed and updated ***<PM-17_ODP[02] frequency>***
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-17-Examine	[SELECT FROM: Controlled unclassified information policy; controlled unclassified information procedures; other relevant documents or records.].
	PM-17-Interview	[SELECT FROM: Organizational personnel with controlled unclassified information responsibilities; organizational personnel with information security responsibilities.].

PM-18	PRIVACY PROGRAM PLAN	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-18_ODP	***the frequency of updates to the privacy program plan is defined;***
	PM-18a.[01]	an organization-wide privacy program plan that provides an overview of the agency's privacy program is developed;
	PM-18a.01[01]	the privacy program plan includes a description of the structure of the privacy program;
	PM-18a.01[02]	the privacy program plan includes a description of the resources dedicated to the privacy program;
	PM-18a.02[01]	the privacy program plan provides an overview of the requirements for the privacy program;
	PM-18a.02[02]	the privacy program plan provides a description of the privacy program management controls in place or planned for meeting the requirements of the privacy program;
	PM-18a.02[03]	the privacy program plan provides a description of common controls in place or planned for meeting the requirements of the privacy program;
	PM-18a.03[01]	the privacy program plan includes the role of the senior agency official for privacy;

PM-18	PRIVACY PROGRAM PLAN	
	PM-18a.03[02]	the privacy program plan includes the identification and assignment of the roles of other privacy officials and staff and their responsibilities;
	PM-18a.04[01]	the privacy program plan describes management commitment;
	PM-18a.04[02]	the privacy program plan describes compliance;
	PM-18a.04[03]	the privacy program plan describes the strategic goals and objectives of the privacy program;
	PM-18a.05	the privacy program plan reflects coordination among organizational entities responsible for the different aspects of privacy;
	PM-18a.06	the privacy program plan is approved by a senior official with responsibility and accountability for the privacy risk being incurred by organizational operations (including, mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;
	PM-18a.[02]	the privacy program plan is disseminated;
	PM-18b.[01]	the privacy program plan is updated ***<PM-18_ODP frequency>***;
	PM-18b.[02]	the privacy program plan is updated to address changes in federal privacy laws and policies;
	PM-18b.[03]	the privacy program plan is updated to address organizational changes;
	PM-18b.[04]	the privacy program plan is updated to address problems identified during plan implementation or privacy control assessments.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-18-Examine	[SELECT FROM: Privacy program plan; procedures addressing program plan development and implementation; procedures addressing program plan reviews, updates, and approvals; procedures addressing coordination of the program plan with relevant entities; records of program plan reviews, updates, and approvals; other relevant documents or records].
	PM-18-Interview	[SELECT FROM: Organizational personnel with privacy program planning and plan implementation responsibilities; organizational personnel with privacy responsibilities].

PM-19	PRIVACY PROGRAM LEADERSHIP ROLE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-19[01]	a senior agency official for privacy with authority, mission, accountability, and resources is appointed;
	PM-19[02]	the senior agency official for privacy coordinates applicable privacy requirements;
	PM-19[03]	the senior agency official for privacy develops applicable privacy requirements;
	PM-19[04]	the senior agency official for privacy implements applicable privacy requirements;
	PM-19[05]	the senior agency official for privacy manages privacy risks through the organization-wide privacy program.

PM-19	PRIVACY PROGRAM LEADERSHIP ROLE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-19-Examine	[SELECT FROM: Privacy program documents, including policies, procedures, plans, and reports; public privacy notices, including Federal Register notices; privacy impact assessments; privacy risk assessments; Privacy Act statements; system of records notices; computer matching agreements and notices; contracts, information sharing agreements, and memoranda of understanding; governing requirements, including laws, executive orders, regulations, standards, and guidance; other relevant documents or records].
	PM-19-Interview	[SELECT FROM: Organizational personnel with privacy program planning and plan implementation responsibilities; organizational personnel with privacy responsibilities; senior agency official for privacy; privacy officials].

PM-20	DISSEMINATION OF PRIVACY PROGRAM INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-20[01]	a central resource webpage is maintained on the organization's principal public website;
	PM-20[02]	the webpage serves as a central source of information about the organization's privacy program;
	PM-20a.[01]	the webpage ensures that the public has access to information about organizational privacy activities;
	PM-20a.[02]	the webpage ensures that the public can communicate with its senior agency official for privacy;
	PM-20b.[01]	the webpage ensures that organizational privacy practices are publicly available;
	PM-20b.[02]	the webpage ensures that organizational privacy reports are publicly available;
	PM-20c.	the webpage employs publicly facing email addresses and/or phone numbers to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-20-Examine	[SELECT FROM: Public website; publicly posted privacy program documents, including policies, procedures, plans, and reports; position description of the senior agency official for privacy; public privacy notices, including Federal Register notices; privacy impact assessments; privacy risk assessments; Privacy Act statements and system of records notices; computer matching agreements and notices; other relevant documents or records].
	PM-20-Interview	[SELECT FROM: Organizational personnel with privacy program information dissemination responsibilities; organizational personnel with privacy responsibilities].
	PM-20-Test	[SELECT FROM: Location, access, availability, and functionality of privacy resource webpage].

PM-20(01)	DISSEMINATION OF PRIVACY PROGRAM INFORMATION | PRIVACY POLICIES ON WEBSITES, APPLICATIONS, AND DIGITAL SERVICES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-20(01)[01]	privacy policies are developed and posted on all external-facing websites;
	PM-20(01)[02]	privacy policies are developed and posted on all mobile applications;
	PM-20(01)[03]	privacy policies are developed and posted on all other digital services;
	PM-20(01)(a)[01]	the privacy policies are written in plain language;
	PM-20(01)(a)[02]	the privacy policies are organized in a way that is easy to understand and navigate;
	PM-20(01)(b)[01]	the privacy policies provide the information needed by the public to make an informed decision about whether to interact with the organization;
	PM-20(01)(b)[02]	the privacy policies provide the information needed by the public to make an informed decision about how to interact with the organization;
	PM-20(01)(c)[01]	the privacy policies are updated whenever the organization makes a substantive change to the practices it describes;
	PM-20(01)(c)[02]	the privacy policies include a time/date stamp to inform the public of the date of the most recent changes.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-20(01)-Examine	[SELECT FROM: Privacy program plan; privacy policies on the agency website, mobile applications, and/or other digital services].
	PM-20(01)-Interview	[SELECT FROM: Organizational personnel with privacy program information dissemination responsibilities; organizational personnel with privacy responsibilities].
	PM-20(01)-Test	[SELECT FROM: Organizational procedures and practices for authorizing, conducting, managing, and reviewing personally identifiable information processing; organizational procedures and practices for disseminating privacy program information; mechanisms supporting the dissemination of privacy program information].

PM-21	ACCOUNTING OF DISCLOSURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-21a.	an accurate accounting of disclosures of personally identifiable information is developed and maintained;
	PM-21a.01[01]	the accounting includes the date of each disclosure;
	PM-21a.01[02]	the accounting includes the nature of each disclosure;
	PM-21a.01[03]	the accounting includes the purpose of each disclosure;
	PM-21a.02[01]	the accounting includes the name of the individual or organization to whom the disclosure was made;

PM-21	ACCOUNTING OF DISCLOSURES	
	PM-21a.02[02]	the accounting includes the address or other contact information of the individual or organization to whom the disclosure was made;
	PM-21b.	the accounting of disclosures is retained for the length of time that the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer;
	PM-21c.	the accounting of disclosures is made available to the individual to whom the personally identifiable information relates upon request.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-21-Examine	[SELECT FROM: Privacy program plan; disclosure policies and procedures; records of disclosures; audit logs; Privacy Act policies and procedures; system of records notice; Privacy Act exemption rules.].
	PM-21-Interview	[SELECT FROM: Organizational personnel with privacy program responsibilities; organizational personnel with privacy responsibilities.].
	PM-21-Test	[SELECT FROM: Organizational processes for disclosures; mechanisms supporting the accounting of disclosures, including commercial services that provide notifications and alerts.].

PM-22	PERSONALLY IDENTIFIABLE INFORMATION QUALITY MANAGEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-22[01]	organization-wide policies for personally identifiable information quality management are developed and documented;
	PM-22[02]	organization-wide procedures for personally identifiable information quality management are developed and documented;
	PM-22a.[01]	the policies address reviewing the accuracy of personally identifiable information across the information life cycle;
	PM-22a.[02]	the policies address reviewing the relevance of personally identifiable information across the information life cycle;
	PM-22a.[03]	the policies address reviewing the timeliness of personally identifiable information across the information life cycle;
	PM-22a.[04]	the policies address reviewing the completeness of personally identifiable information across the information life cycle;
	PM-22a.[05]	the procedures address reviewing the accuracy of personally identifiable information across the information life cycle;
	PM-22a.[06]	the procedures address reviewing the relevance of personally identifiable information across the information life cycle;
	PM-22a.[07]	the procedures address reviewing the timeliness of personally identifiable information across the information life cycle;
	PM-22a.[08]	the procedures address reviewing the completeness of personally identifiable information across the information life cycle;

PM-22	PERSONALLY IDENTIFIABLE INFORMATION QUALITY MANAGEMENT	
	PM-22b.[01]	the policies address correcting or deleting inaccurate or outdated personally identifiable information;
	PM-22b.[02]	the procedures address correcting or deleting inaccurate or outdated personally identifiable information;
	PM-22c.[01]	the policies address disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities;
	PM-22c.[02]	the procedures address disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities;
	PM-22d.[01]	the policies address appeals of adverse decisions on correction or deletion requests;
	PM-22d.[02]	the procedures address appeals of adverse decisions on correction or deletion requests.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-22-Examine	[SELECT FROM: Privacy program plan; policies and procedures addressing personally identifiable information quality management, information life cycle documentation, and sample notices of correction or deletion; records of monitoring PII quality management practices; documentation of reviews and updates of policies and procedures].
	PM-22-Interview	[SELECT FROM: Organizational personnel with privacy program information dissemination responsibilities; organizational personnel with privacy responsibilities].
	PM-22-Test	[SELECT FROM: [Organizational processes for data quality and personally identifiable information quality management procedures; mechanisms supporting and/or implementing quality management requirements].

PM-23	DATA GOVERNANCE BODY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-23_ODP[01]	***the roles of a Data Governance Body are defined;***
	PM-23_ODP[02]	***the responsibilities of a Data Governance Body are defined;***
	PM-23	a Data Governance Body consisting of ***<PM-23_ODP[01] roles>*** with ***<PM-23_ODP[02] responsibilities>*** is established.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-23-Examine	[SELECT FROM: Privacy program plan; documentation relating to the Data Governance Body, including documents establishing such a body, its charter of operations, and any plans and reports; records of board meetings and decisions; records of requests to review data; policies, procedures, and standards that facilitate data governance].
	PM-23-Interview	[SELECT FROM: Officials serving on the Data Governance Body (e.g., chief information officer, senior agency information security officer, and senior agency official for privacy)].

PM-24	DATA INTEGRITY BOARD	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-24	a Data Integrity Board is established;
	PM-24a.	the Data Integrity Board reviews proposals to conduct or participate in a matching program;
	PM-24b.	the Data Integrity Board conducts an annual review of all matching programs in which the agency has participated.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-24-Examine	[SELECT FROM: Privacy program plan; privacy program documents relating to the Data Integrity Board, including documents establishing the board, its charter of operations, and any plans and reports; computer matching agreements and notices; information sharing agreements; memoranda of understanding; records documenting annual reviews; governing requirements, including laws, executive orders, regulations, standards, and guidance].
	PM-24-Interview	[SELECT FROM: members of the Data Integrity Board (e.g., the chief information officer, senior information security officer, senior agency official for privacy, and agency Inspector General)].

PM-25	MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION USED IN TESTING, TRAINING, AND RESEARCH	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-25_ODP[01]	***the frequency for reviewing policies that address the use of personally identifiable information for internal testing, training, and research is defined;***
	PM-25_ODP[02]	***the frequency for updating policies that address the use of personally identifiable information for internal testing, training, and research is defined;***
	PM-25_ODP[03]	***the frequency for reviewing procedures that address the use of personally identifiable information for internal testing, training, and research is defined;***
	PM-25_ODP[04]	***the frequency for updating procedures that address the use of personally identifiable information for internal testing, training, and research is defined;***
	PM-25a.[01]	policies that address the use of personally identifiable information for internal testing are developed and documented;
	PM-25a.[02]	policies that address the use of personally identifiable information for internal training are developed and documented;
	PM-25a.[03]	policies that address the use of personally identifiable information for internal research are developed and documented;
	PM-25a.[04]	procedures that address the use of personally identifiable information for internal testing are developed and documented;
	PM-25a.[05]	procedures that address the use of personally identifiable information for internal training are developed and documented;

PM-25	MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION USED IN TESTING, TRAINING, AND RESEARCH	
	PM-25a.[06]	procedures that address the use of personally identifiable information for internal research are developed and documented;
	PM-25a.[07]	policies that address the use of personally identifiable information for internal testing, are implemented;
	PM-25a.[08]	policies that address the use of personally identifiable information for training are implemented;
	PM-25a.[09]	policies that address the use of personally identifiable information for research are implemented;
	PM-25a.[10]	procedures that address the use of personally identifiable information for internal testing are implemented;
	PM-25a.[11]	procedures that address the use of personally identifiable information for training are implemented;
	PM-25a.[12]	procedures that address the use of personally identifiable information for research are implemented;
	PM-25b.[01]	the amount of personally identifiable information used for internal testing purposes is limited or minimized;
	PM-25b.[02]	the amount of personally identifiable information used for internal training purposes is limited or minimized;
	PM-25b.[03]	the amount of personally identifiable information used for internal research purposes is limited or minimized;
	PM-25c.[01]	the required use of personally identifiable information for internal testing is authorized;
	PM-25c.[02]	the required use of personally identifiable information for internal training is authorized;
	PM-25c.[03]	the required use of personally identifiable information for internal research is authorized;
	PM-25d.[01]	policies are reviewed ***<PM-25_ODP[01] frequency>***;
	PM-25d.[02]	policies are updated ***<PM-25_ODP[02] frequency>***;
	PM-25d.[03]	procedures are reviewed ***<PM-25_ODP[03] frequency>***;
	PM-25d.[04]	procedures are updated ***<PM-25_ODP[04] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-25-Examine	[SELECT FROM: Privacy program plan; policies and procedures for the minimization of personally identifiable information used in testing, training, and research; documentation supporting policy implementation (e.g., templates for testing, training, and research; privacy threshold analysis; privacy risk assessment); data sets used for testing, training, and research].
	PM-25-Interview	[SELECT FROM: Organizational personnel with privacy program responsibilities; organizational personnel with privacy responsibilities; system developers; personnel with IRB responsibilities].

PM-25	MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION USED IN TESTING, TRAINING, AND RESEARCH	
	PM-25-Test	[SELECT FROM: Organizational processes for data quality and personally identifiable information management; mechanisms supporting data quality management and personally identifiable information management to minimize the use of personally identifiable information].

PM-26	COMPLAINT MANAGEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-26_ODP[01]	***the time period in which complaints (including concerns or questions) from individuals are to be reviewed is defined;***
	PM-26_ODP[02]	***the time period in which complaints (including concerns or questions) from individuals are to be addressed is defined;***
	PM-26_ODP[03]	***the time period for acknowledging the receipt of complaints is defined;***
	PM-26_ODP[04]	***the time period for responding to complaints is defined;***
	PM-26[01]	a process for receiving complaints, concerns, or questions from individuals about organizational security and privacy practices is implemented;
	PM-26[02]	a process for responding to complaints, concerns, or questions from individuals about organizational security and privacy practices is implemented;
	PM-26a.[01]	the complaint management process includes mechanisms that are easy to use by the public;
	PM-26a.[02]	the complaint management process includes mechanisms that are readily accessible by the public;
	PM-26b.	the complaint management process includes all information necessary for successfully filing complaints;
	PM-26c.[01]	the complaint management process includes tracking mechanisms to ensure that all complaints are reviewed within ***<PM-26_ODP[01] time period>***;
	PM-26c.[02]	the complaint management process includes tracking mechanisms to ensure that all complaints are addressed within ***<PM-26_ODP[02] time period>***;
	PM-26d.	the complaint management process includes acknowledging the receipt of complaints, concerns, or questions from individuals within ***<PM-26_ODP[03] time period>***;
	PM-26e.	the complaint management process includes responding to complaints, concerns, or questions from individuals within ***<PM-26_ODP[04] time period>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-26-Examine	[SELECT FROM: Privacy program plan; procedures addressing complaint management; complaint documentation; procedures addressing the reviews of complaints; other relevant documents or records].
	PM-26-Interview	[SELECT FROM: Organizational personnel with privacy program responsibilities; organizational personnel with privacy responsibilities].

PM-26	COMPLAINT MANAGEMENT	
	PM-26-Test	[SELECT FROM: Organizational processes for complaint management; mechanisms supporting complaint management; tools used by the public to submit complaints, concerns, and questions (e.g., telephone, hotline, email, or web-based forms].

PM-27	PRIVACY REPORTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-27_ODP[01]	***privacy reports are defined;***
	PM-27_ODP[02]	***privacy oversight bodies are defined;***
	PM-27_ODP[03]	***officials responsible for monitoring privacy program compliance are defined;***
	PM-27_ODP[04]	***the frequency for reviewing and updating privacy reports is defined;***
	PM-27a.	***<PM-27_ODP[01] privacy reports>*** are developed;
	PM-27a.01	the privacy reports are disseminated to ***<PM-27_ODP[02] oversight bodies>*** to demonstrate accountability with statutory, regulatory, and policy privacy mandates;
	PM-27a.02[01]	the privacy reports are disseminated to ***<PM-27_ODP[03] officials>***;
	PM-27a.02[02]	the privacy reports are disseminated to other personnel responsible for monitoring privacy program compliance;
	PM-27b.	the privacy reports are reviewed and updated ***<PM-27_ODP[04] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-27-Examine	[SELECT FROM: Privacy program plan; internal and external privacy reports; privacy program plan; annual senior agency official for privacy reports to OMB; reports to Congress required by law, regulation, or policy, including internal policies; records documenting the dissemination of reports to oversight bodies and officials responsible for monitoring privacy program compliance; records of review and updates of privacy reports.].
	PM-27-Interview	[SELECT FROM: Organizational personnel with privacy program responsibilities; organizational personnel with privacy responsibilities; legal counsel.].

PM-28	RISK FRAMING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-28_ODP[01]	***the personnel to receive the results of risk framing activities is/are defined;***
	PM-28_ODP[02]	***the frequency for reviewing and updating risk framing considerations is defined;***
	PM-28a.01[01]	assumptions affecting risk assessments are identified and documented;
	PM-28a.01[02]	assumptions affecting risk responses are identified and documented;
	PM-28a.01[03]	assumptions affecting risk monitoring are identified and documented;

PM-28	RISK FRAMING	
	PM-28a.02[01]	constraints affecting risk assessments are identified and documented;
	PM-28a.02[02]	constraints affecting risk responses are identified and documented;
	PM-28a.02[03]	constraints affecting risk monitoring are identified and documented;
	PM-28a.03[01]	priorities considered by the organization for managing risk are identified and documented;
	PM-28a.03[02]	trade-offs considered by the organization for managing risk are identified and documented;
	PM-28a.04	organizational risk tolerance is identified and documented;
	PM-28b.	the results of risk framing activities are distributed to ***<PM-28_ODP[01] personnel>***;
	PM-28c.	risk framing considerations are reviewed and updated ***<PM-28_ODP[02] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-28-Examine	[SELECT FROM: Information security program plan; privacy program plan; supply chain risk management strategy; documentation of risk framing activities; policies and procedures for risk framing activities; risk management strategy].
	PM-28-Interview	[SELECT FROM: Organizational personnel (including mission, business, and system owners or stewards; authorizing officials; senior agency information security officer; senior agency official for privacy; and senior accountable official for risk management)].
	PM-28-Test	[SELECT FROM: Organizational procedures and practices for authorizing, conducting, managing, and reviewing personally identifiable information processing; organizational processes for risk framing; mechanisms supporting the development, review, update, and approval of risk framing].

PM-29	RISK MANAGEMENT PROGRAM LEADERSHIP ROLES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-29a.[01]	a Senior Accountable Official for Risk Management is appointed;
	PM-29a.[02]	a Senior Accountable Official for Risk Management aligns information security and privacy management processes with strategic, operational, and budgetary planning processes;
	PM-29b.[01]	a Risk Executive (function) is established;
	PM-29b.[02]	a Risk Executive (function) views and analyzes risk from an organization-wide perspective;
	PM-29b.[03]	a Risk Executive (function) ensures that the management of risk is consistent across the organization.

PM-29	RISK MANAGEMENT PROGRAM LEADERSHIP ROLES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-29-Examine	[SELECT FROM: Information security program plan; privacy program plan; risk management strategy; supply chain risk management strategy; documentation of appointment, roles, and responsibilities of a Senior Accountable Official for Risk Management; documentation of actions taken by the Official; documentation of the establishment, policies, and procedures of a Risk Executive (function)].
	PM-29-Interview	[SELECT FROM: Senior Accountable Official for Risk Management; chief information officer; senior agency information security officer; senior agency official for privacy; organizational personnel with information security and privacy program responsibilities].

PM-30	SUPPLY CHAIN RISK MANAGEMENT STRATEGY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-30_ODP	***the frequency for reviewing and updating the supply chain risk management strategy is defined;***
	PM-30a.[01]	an organization-wide strategy for managing supply chain risks is developed;
	PM-30a.[02]	the supply chain risk management strategy addresses risks associated with the development of systems;
	PM-30a.[03]	the supply chain risk management strategy addresses risks associated with the development of system components;
	PM-30a.[04]	the supply chain risk management strategy addresses risks associated with the development of system services;
	PM-30a.[05]	the supply chain risk management strategy addresses risks associated with the acquisition of systems;
	PM-30a.[06]	the supply chain risk management strategy addresses risks associated with the acquisition of system components;
	PM-30a.[07]	the supply chain risk management strategy addresses risks associated with the acquisition of system services;
	PM-30a.[08]	the supply chain risk management strategy addresses risks associated with the maintenance of systems;
	PM-30a.[09]	the supply chain risk management strategy addresses risks associated with the maintenance of system components;
	PM-30a.[10]	the supply chain risk management strategy addresses risks associated with the maintenance of system services;
	PM-30a.[11]	the supply chain risk management strategy addresses risks associated with the disposal of systems;
	PM-30a.[12]	the supply chain risk management strategy addresses risks associated with the disposal of system components;
	PM-30a.[13]	the supply chain risk management strategy addresses risks associated with the disposal of system services;

PM-30	SUPPLY CHAIN RISK MANAGEMENT STRATEGY	
	PM-30b.	the supply chain risk management strategy is implemented consistently across the organization;
	PM-30c.	the supply chain risk management strategy is reviewed and updated ***<PM-30_ODP frequency>*** or as required to address organizational changes.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-30-Examine	[SELECT FROM: Supply chain risk management strategy; organizational risk management strategy; enterprise risk management documents; other relevant documents or records].
	PM-30-Interview	[SELECT FROM: Organizational personnel with supply chain risk management responsibilities; organizational personnel with information security responsibilities; organizational personnel with acquisition responsibilities; organizational personnel with enterprise risk management responsibilities].

PM-30(01)	SUPPLY CHAIN RISK MANAGEMENT STRATEGY | SUPPLIERS OF CRITICAL OR MISSION-ESSENTIAL ITEMS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-30(01)[01]	suppliers of critical or mission-essential technologies, products, and services are identified;
	PM-30(01)[02]	suppliers of critical or mission-essential technologies, products, and services are prioritized;
	PM-30(01)[03]	suppliers of critical or mission-essential technologies, products, and services are assessed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-30(01)-Examine	[SELECT FROM: Supply chain risk management strategy; organization-wide risk management strategy; enterprise risk management documents; inventory records or suppliers; assessment and prioritization documentation; critical or mission-essential technologies, products, and service documents or records; other relevant documents or records].
	PM-30(01)-Interview	[SELECT FROM: Organizational personnel with supply chain risk management responsibilities; organizational personnel with information security responsibilities; organizational personnel with acquisition responsibilities; organizational personnel with enterprise risk management responsibilities].
	PM-30(01)-Test	[SELECT FROM: Organizational processes for identifying, prioritizing, and assessing critical or mission-essential technologies, products, and services; organizational processes for maintaining an inventory of suppliers; organizational process for associating suppliers with critical or mission-essential technologies, products, and services].

PM-31	CONTINUOUS MONITORING STRATEGY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-31_ODP[01]	***the metrics for organization-wide continuous monitoring are defined;***
	PM-31_ODP[02]	***the frequency for monitoring is defined;***
	PM-31_ODP[03]	***the frequency for assessing control effectiveness is defined;***
	PM-31_ODP[04]	***the personnel or roles for reporting the security status of organizational systems to is/are defined;***
	PM-31_ODP[05]	***the personnel or roles for reporting the privacy status of organizational systems to is/are defined;***
	PM-31_ODP[06]	***the frequency at which to report the security status of organizational systems is defined;***
	PM-31_ODP[07]	***the frequency at which to report the privacy status of organizational systems is defined;***
	PM-31	an organization-wide continuous monitoring strategy is developed;
	PM-31a.	continuous monitoring programs are implemented that include establishing ***<PM-31_ODP[01] metrics>*** to be monitored;
	PM-31b.[01]	continuous monitoring programs are implemented that establish ***<PM-31_ODP[02] frequency>*** for monitoring;
	PM-31b.[02]	continuous monitoring programs are implemented that establish ***<PM-31_ODP[03] frequency>*** for assessment of control effectiveness;
	PM-31c.	continuous monitoring programs are implemented that include monitoring ***<PM-31_ODP[01] metrics>*** on an ongoing basis in accordance with the continuous monitoring strategy;
	PM-31d.[01]	continuous monitoring programs are implemented that include correlating information generated by control assessments and monitoring;
	PM-31d.[02]	continuous monitoring programs are implemented that include analyzing information generated by control assessments and monitoring;
	PM-31e.[01]	continuous monitoring programs are implemented that include response actions to address the analysis of control assessment information;
	PM-31e.[02]	continuous monitoring programs are implemented that include response actions to address the analysis of monitoring information;
	PM-31f.[01]	continuous monitoring programs are implemented that include reporting the security status of organizational systems to ***<PM-31_ODP[04] personnel or roles>*** ***<PM-31_ODP[06] frequency>***;
	PM-31f.[02]	continuous monitoring programs are implemented that include reporting the privacy status of organizational systems to ***<PM-31_ODP[05] personnel or roles>*** ***<PM-31_ODP[07] frequency>***.

PM-31	CONTINUOUS MONITORING STRATEGY	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-31-Examine	[SELECT FROM: Information security program plan; privacy program plan; supply chain risk management plan; continuous monitoring strategy; risk management strategy; information security continuous monitoring program documentation, reporting, metrics, and artifacts; information security continuous monitoring program assessment documentation, reporting, metrics, and artifacts; assessment and authorization policy; procedures addressing the continuous monitoring of controls; privacy program continuous monitoring documentation, reporting, metrics, and artifacts; continuous monitoring program records, security, and privacy impact analyses; status reports; risk response documentation; other relevant documents or records.].
	PM-31-Interview	[SELECT FROM: Senior Accountable Official for Risk Management; chief information officer; senior agency information security officer; senior agency official for privacy; organizational personnel with information security, privacy, and supply chain risk management program responsibilities].
	PM-31-Test	[SELECT FROM: Organizational procedures and mechanisms used for information security, privacy, and supply chain continuous monitoring].

PM-32	PURPOSING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PM-32_ODP	***the systems or system components supporting mission-essential services or functions are defined;***
	PM-32	***<PM-32_ODP systems or system components>*** supporting mission-essential services or functions are analyzed to ensure that the information resources are being used in a manner that is consistent with their intended purpose.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PM-32-Examine	[SELECT FROM: Information security program plan; privacy program plan; list of essential services and functions; organizational analysis of information resources; risk management strategy; other relevant documents or records.].
	PM-32-Interview	[SELECT FROM: Organizational personnel with information security, privacy, and supply chain risk management program responsibilities].

4.14 PERSONNEL SECURITY

PS-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PS-01_ODP[01]	***personnel or roles to whom the personnel security policy is to be disseminated is/are defined;***
	PS-01_ODP[02]	***personnel or roles to whom the personnel security procedures are to be disseminated is/are defined;***
	PS-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	PS-01_ODP[04]	***an official to manage the personnel security policy and procedures is defined;***
	PS-01_ODP[05]	***the frequency at which the current personnel security policy is reviewed and updated is defined;***
	PS-01_ODP[06]	***events that would require the current personnel security policy to be reviewed and updated are defined;***
	PS-01_ODP[07]	***the frequency at which the current personnel security procedures are reviewed and updated is defined;***
	PS-01_ODP[08]	***events that would require the personnel security procedures to be reviewed and updated are defined;***
	PS-01a.[01]	a personnel security policy is developed and documented;
	PS-01a.[02]	the personnel security policy is disseminated to ***<PS-01_ODP[01] personnel or roles>***;
	PS-01a.[03]	personnel security procedures to facilitate the implementation of the personnel security policy and associated personnel security controls are developed and documented;
	PS-01a.[04]	the personnel security procedures are disseminated to ***<PS-01_ODP[02] personnel or roles>***;
	PS-01a.01(a)[01]	the ***<PS-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** personnel security policy addresses purpose;
	PS-01a.01(a)[02]	the ***<PS-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** personnel security policy addresses scope;
	PS-01a.01(a)[03]	the ***<PS-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** personnel security policy addresses roles;
	PS-01a.01(a)[04]	the ***<PS-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** personnel security policy addresses responsibilities;
	PS-01a.01(a)[05]	the ***<PS-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** personnel security policy addresses management commitment;
	PS-01a.01(a)[06]	the ***<PS-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** personnel security policy addresses coordination among organizational entities;
	PS-01a.01(a)[07]	the ***<PS-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** personnel security policy addresses compliance;

PS-01	POLICY AND PROCEDURES	
	PS-01a.01(b)	the ***<PS-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** personnel security policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines;
	PS-01b.	the ***<PS-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the personnel security policy and procedures;
	PS-01c.01[01]	the current personnel security policy is reviewed and updated ***<PS-01_ODP[05] frequency>***;
	PS-01c.01[02]	the current personnel security policy is reviewed and updated following ***<PS-01_ODP[06] events>***;
	PS-01c.02[01]	the current personnel security procedures are reviewed and updated ***<PS-01_ODP[07] frequency>***;
	PS-01c.02[02]	the current personnel security procedures are reviewed and updated following ***<PS-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PS-01-Examine	[SELECT FROM: Personnel security policy; personnel security procedures; system security plan; privacy plan; risk management strategy documentation; audit findings; other relevant documents or records].
	PS-01-Interview	[SELECT FROM: Organizational personnel with personnel security responsibilities; organizational personnel with information security responsibilities].

PS-02	POSITION RISK DESIGNATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PS-02_ODP	***the frequency at which to review and update position risk designations is defined;***
	PS-02a.	a risk designation is assigned to all organizational positions;
	PS-02b.	screening criteria are established for individuals filling organizational positions;
	PS-02c.	position risk designations are reviewed and updated ***<PS-02_ODP frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PS-02-Examine	[SELECT FROM: Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; list of risk designations for organizational positions; records of position risk designation reviews and updates; system security plan; other relevant documents or records].
	PS-02-Interview	[SELECT FROM: Organizational personnel with personnel security responsibilities; organizational personnel with information security responsibilities].
	PS-02-Test	[SELECT FROM: Organizational processes for assigning, reviewing, and updating position risk designations; organizational processes for establishing screening criteria].

PS-03	PERSONNEL SCREENING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PS-03_ODP[01]	***conditions requiring rescreening of individuals are defined;***
	PS-03_ODP[02]	***the frequency of rescreening individuals where it is so indicated is defined;***
	PS-03a.	individuals are screened prior to authorizing access to the system;
	PS-03b.[01]	individuals are rescreened in accordance with ***<PS-03_ODP[01] conditions requiring rescreening>***;
	PS-03b.[02]	where rescreening is so indicated, individuals are rescreened ***<PS-03_ODP[02] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PS-03-Examine	[SELECT FROM: Personnel security policy; procedures addressing personnel screening; records of screened personnel; system security plan; other relevant documents or records].
	PS-03-Interview	[SELECT FROM: Organizational personnel with personnel security responsibilities; organizational personnel with information security responsibilities].
	PS-03-Test	[SELECT FROM: Organizational processes for personnel screening].

PS-03(01)	PERSONNEL SCREENING | CLASSIFIED INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PS-03(01)[01]	individuals accessing a system processing, storing, or transmitting classified information are cleared;
	PS-03(01)[02]	individuals accessing a system processing, storing, or transmitting classified information are indoctrinated to the highest classification level of the information to which they have access on the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PS-03(01)-Examine	[SELECT FROM: Personnel security policy; procedures addressing personnel screening; records of screened personnel; system security plan; other relevant documents or records].
	PS-03(01)-Interview	[SELECT FROM: Organizational personnel with personnel security responsibilities; organizational personnel with information security responsibilities].
	PS-03(01)-Test	[SELECT FROM: Organizational processes for clearing and indoctrinating personnel for access to classified information].

PS-03(02)	PERSONNEL SCREENING | FORMAL INDOCTRINATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PS-03(02)	individuals accessing a system processing, storing, or transmitting types of classified information that require formal indoctrination are formally indoctrinated for all of the relevant types of information to which they have access on the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PS-03(02)-Examine	[SELECT FROM: Personnel security policy; procedures addressing personnel screening; indoctrination documents; records of screened personnel; system security plan; other relevant documents or records].
	PS-03(02)-Interview	[SELECT FROM: Organizational personnel with personnel security responsibilities; organizational personnel with information security responsibilities].
	PS-03(02)-Test	[SELECT FROM: Organizational processes for formal indoctrination for all relevant types of information to which personnel have access].

PS-03(03)	PERSONNEL SCREENING | INFORMATION REQUIRING SPECIAL PROTECTIVE MEASURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PS-03(03)_ODP	***additional personnel screening criteria to be satisfied for individuals accessing a system processing, storing, or transmitting information requiring special protection are defined;***
	PS-03(03)(a)	individuals accessing a system processing, storing, or transmitting information requiring special protection have valid access authorizations that are demonstrated by assigned official government duties;
	PS-03(03)(b)	individuals accessing a system processing, storing, or transmitting information requiring special protection satisfy ***<PS-03(03)_ODP additional personnel screening criteria>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PS-03(03)-Examine	[SELECT FROM: Personnel security policy; access control policy, procedures addressing personnel screening; records of screened personnel; screening criteria; records of access authorizations; system security plan; other relevant documents or records].
	PS-03(03)-Interview	[SELECT FROM: Organizational personnel with personnel security responsibilities; organizational personnel with information security responsibilities].
	PS-03(03)-Test	[SELECT FROM: Organizational processes for ensuring valid access authorizations for information requiring special protection; organizational process for additional personnel screening for information requiring special protection].

PS-03(04)	PERSONNEL SCREENING | CITIZENSHIP REQUIREMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PS-03(04)_ODP[01]	***information types that are processed, stored, or transmitted by a system that require individuals accessing the system to meet <PS-03(04)_ODP[02] citizenship requirements> are defined;***
	PS-03(04)_ODP[02]	***citizenship requirements to be met by individuals to access a system processing, storing, or transmitting information are defined;***
	PS-03(04)	individuals accessing a system processing, storing, or transmitting ***<PS-03(04)_ODP[01] information types>*** meet ***<PS-03(04)_ODP[02] citizenship requirements>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PS-03(04)-Examine	[SELECT FROM: Personnel security policy; access control policy, procedures addressing personnel screening; records of screened personnel; screening criteria; records of access authorizations; system security plan; other relevant documents or records].
	PS-03(04)-Interview	[SELECT FROM: Organizational personnel with personnel security responsibilities; organizational personnel with information security responsibilities].
	PS-03(04)-Test	[SELECT FROM: Organizational processes for ensuring valid access authorizations for information requiring citizenship; organizational process for additional personnel screening for information requiring citizenship].

PS-04	PERSONNEL TERMINATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PS-04_ODP[01]	***a time period within which to disable system access is defined;***
	PS-04_ODP[02]	***information security topics to be discussed when conducting exit interviews are defined;***
	PS-04a.	upon termination of individual employment, system access is disabled within ***<PS-04_ODP[01] time period>***;
	PS-04b.	upon termination of individual employment, any authenticators and credentials are terminated or revoked;
	PS-04c.	upon termination of individual employment, exit interviews that include a discussion of ***<PS-04_ODP[02] information security topics>*** are conducted;
	PS-04d.	upon termination of individual employment, all security-related organizational system-related property is retrieved;
	PS-04e.	upon termination of individual employment, access to organizational information and systems formerly controlled by the terminated individual are retained.

PS-04	PERSONNEL TERMINATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PS-04-Examine	[SELECT FROM: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of system accounts; records of terminated or revoked authenticators/credentials; records of exit interviews; system security plan; other relevant documents or records].
	PS-04-Interview	[SELECT FROM: Organizational personnel with personnel security responsibilities; organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities].
	PS-04-Test	[SELECT FROM: Organizational processes for personnel termination; mechanisms supporting and/or implementing personnel termination notifications; mechanisms for disabling system access/revoking authenticators].

PS-04(01)	PERSONNEL TERMINATION | POST-EMPLOYMENT REQUIREMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PS-04(01)(a)	terminated individuals are notified of applicable, legally binding post-employment requirements for the protection of organizational information;
	PS-04(01)(b)	terminated individuals are required to sign an acknowledgement of post-employment requirements as part of the organizational termination process.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PS-04(01)-Examine	[SELECT FROM: Personnel security policy; procedures addressing personnel termination; signed post-employment acknowledgement forms; list of applicable, legally binding post-employment requirements; system security plan; other relevant documents or records].
	PS-04(01)-Interview	[SELECT FROM: Organizational personnel with personnel security responsibilities; organizational personnel with information security responsibilities].
	PS-04(01)-Test	[SELECT FROM: Organizational processes for post-employment requirements].

PS-04(02)	PERSONNEL TERMINATION | AUTOMATED ACTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PS-04(02)_ODP[01]	***automated mechanisms to notify personnel or roles of individual termination actions and/or to disable access to system resources are defined;***
	PS-04(02)_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {notify <PS-04(02)_ODP[03] personnel or roles> of individual termination actions; disable access to system resources};***
	PS-04(02)_ODP[03]	***personnel or roles to be notified upon termination of an individual is/are defined (if selected);***

PS-04(02)	PERSONNEL TERMINATION | AUTOMATED ACTIONS	
	PS-04(02)	***<PS-04(02)_ODP[01] automated mechanisms>*** are used to ***<PS-04(02)_ODP[02] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PS-04(02)-Examine	[SELECT FROM: Personnel security policy; procedures addressing personnel termination; system design documentation; system configuration settings and associated documentation; records of personnel termination actions; automated notifications of employee terminations; system security plan; other relevant documents or records].
	PS-04(02)-Interview	[SELECT FROM: Organizational personnel with personnel security responsibilities; organizational personnel with information security responsibilities].
	PS-04(02)-Test	[SELECT FROM: Organizational processes for personnel termination; automated mechanisms supporting and/or implementing personnel termination notifications].

PS-05	PERSONNEL TRANSFER	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PS-05_ODP[01]	***transfer or reassignment actions to be initiated following transfer or reassignment are defined;***
	PS-05_ODP[02]	***the time period within which transfer or reassignment actions must occur following transfer or reassignment is defined;***
	PS-05_ODP[03]	***personnel or roles to be notified when individuals are reassigned or transferred to other positions within the organization is/are defined;***
	PS-05_ODP[04]	***time period within which to notify organization-defined personnel or roles when individuals are reassigned or transferred to other positions within the organization is defined;***
	PS-05a.	the ongoing operational need for current logical and physical access authorizations to systems and facilities are reviewed and confirmed when individuals are reassigned or transferred to other positions within the organization;
	PS-05b.	***<PS-05_ODP[01] transfer or reassignment actions>*** are initiated within ***<PS-05_ODP[02] time period following the formal transfer action>***;
	PS-05c.	access authorization is modified as needed to correspond with any changes in operational need due to reassignment or transfer;
	PS-05d.	***<PS-05_ODP[03] personnel or roles>*** are notified within ***<PS-05_ODP[04] time period>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PS-05-Examine	[SELECT FROM: Personnel security policy; procedures addressing personnel transfer; records of personnel transfer actions; list of system and facility access authorizations; system security plan; other relevant documents or records].
	PS-05-Interview	[SELECT FROM: Organizational personnel with personnel security responsibilities; organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities].

PS-05	PERSONNEL TRANSFER	
	PS-05-Test	[SELECT FROM: Organizational processes for personnel transfer; mechanisms supporting and/or implementing personnel transfer notifications; mechanisms for disabling system access/revoking authenticators].

PS-06	ACCESS AGREEMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PS-06_ODP[01]	***the frequency at which to review and update access agreements is defined;***
	PS-06_ODP[02]	***the frequency at which to re-sign access agreements to maintain access to organizational information is defined;***
	PS-06a.	access agreements are developed and documented for organizational systems;
	PS-06b.	the access agreements are reviewed and updated ***<PS-06_ODP[01] frequency>***;
	PS-06c.01	individuals requiring access to organizational information and systems sign appropriate access agreements prior to being granted access;
	PS-06c.02	individuals requiring access to organizational information and systems re-sign access agreements to maintain access to organizational systems when access agreements have been updated or ***<PS-06_ODP[02] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PS-06-Examine	[SELECT FROM: Personnel security policy; personnel security procedures; procedures addressing access agreements for organizational information and systems; access control policy; access control procedures; access agreements (including non-disclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements); documentation of access agreement reviews, updates, and re-signing; system security plan; privacy plan; other relevant documents or records].
	PS-06-Interview	[SELECT FROM: Organizational personnel with personnel security responsibilities; organizational personnel who have signed/resigned access agreements; organizational personnel with information security and privacy responsibilities].
	PS-06-Test	[SELECT FROM: Organizational processes for reviewing, updating, and re-signing access agreements; mechanisms supporting the reviewing, updating, and re-signing of access agreements].

PS-06(01)	ACCESS AGREEMENTS | INFORMATION REQUIRING SPECIAL PROTECTION
	[WITHDRAWN: Incorporated into PS-03.]

PS-06(02)	ACCESS AGREEMENTS | CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PS-06(02)(a)	access to classified information requiring special protection is granted only to individuals who have a valid access authorization that is demonstrated by assigned official government duties;
	PS-06(02)(b)	access to classified information requiring special protection is granted only to individuals who satisfy associated personnel security criteria;
	PS-06(02)(c)	access to classified information requiring special protection is granted only to individuals who have read, understood, and signed a non-disclosure agreement.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PS-06(02)-Examine	[SELECT FROM: Personnel security policy; procedures addressing access agreements for organizational information and systems; access agreements; access authorizations; personnel security criteria; signed non-disclosure agreements; system security plan; other relevant documents or records].
	PS-06(02)-Interview	[SELECT FROM: Organizational personnel with personnel security responsibilities; organizational personnel who have signed non-disclosure agreements; organizational personnel with information security responsibilities].
	PS-06(02)-Test	[SELECT FROM: Organizational processes for access to classified information requiring special protection].

PS-06(03)	ACCESS AGREEMENTS | POST-EMPLOYMENT REQUIREMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PS-06(03)(a)	individuals are notified of applicable, legally binding post-employment requirements for the protection of organizational information;
	PS-06(03)(b)	individuals are required to sign an acknowledgement of applicable, legally binding post-employment requirements as part of being granted initial access to covered information.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PS-06(03)-Examine	[SELECT FROM: Personnel security policy; procedures addressing access agreements for organizational information and systems; signed post-employment acknowledgement forms; access agreements; list of applicable, legally binding post-employment requirements; system security plan; other relevant documents or records].
	PS-06(03)-Interview	[SELECT FROM: Organizational personnel with personnel security responsibilities; organizational personnel who have signed access agreements that include post-employment requirements; organizational personnel with information security responsibilities].
	PS-06(03)-Test	[SELECT FROM: Organizational processes for post-employment requirements; mechanisms supporting notifications and individual acknowledgements of post-employment requirements].

PS-07	EXTERNAL PERSONNEL SECURITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PS-07_ODP[01]	***personnel or roles to be notified of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges or who have system privileges is/are defined;***
	PS-07_ODP[02]	***time period within which third-party providers are required to notify organization-defined personnel or roles of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges or who have system privileges is defined;***
	PS-07a.	personnel security requirements are established, including security roles and responsibilities for external providers;
	PS-07b.	external providers are required to comply with personnel security policies and procedures established by the organization;
	PS-07c.	personnel security requirements are documented;
	PS-07d.	external providers are required to notify ***<PS-07_ODP[01] personnel or roles>*** of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges or who have system privileges within ***<PS-07_ODP[02] time period>***;
	PS-07e.	provider compliance with personnel security requirements is monitored.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PS-07-Examine	[SELECT FROM: Personnel security policy; procedures addressing external personnel security; list of personnel security requirements; acquisition documents; service-level agreements; compliance monitoring process; system security plan; other relevant documents or records].
	PS-07-Interview	[SELECT FROM: Organizational personnel with personnel security responsibilities; external providers; system/network administrators; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities].
	PS-07-Test	[SELECT FROM: Organizational processes for managing and monitoring external personnel security; mechanisms supporting and/or implementing the monitoring of provider compliance].

PS-08	PERSONNEL SANCTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PS-08_ODP[01]	***personnel or roles to be notified when a formal employee sanctions process is initiated is/are defined;***
	PS-08_ODP[02]	***the time period within which organization-defined personnel or roles must be notified when a formal employee sanctions process is initiated is defined;***
	PS-08a.	a formal sanctions process is employed for individuals failing to comply with established information security and privacy policies and procedures;

PS-08	PERSONNEL SANCTIONS	
	PS-08b.	***<PS-08_ODP[01] personnel or roles>*** is/are notified within ***<PS-08_ODP[02] time period>*** when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PS-08-Examine	[SELECT FROM: Personnel security policy; personnel security procedures; procedures addressing personnel sanctions; access agreements (including non-disclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements); list of personnel or roles to be notified of formal employee sanctions; records or notifications of formal employee sanctions; system security plan; privacy plan; personally identifiable information processing policy; other relevant documents or records].
	PS-08-Interview	[SELECT FROM: Organizational personnel with personnel security responsibilities; legal counsel; organizational personnel with information security and privacy responsibilities].
	PS-08-Test	[SELECT FROM: Organizational processes for managing formal employee sanctions; mechanisms supporting and/or implementing formal employee sanctions notifications].

PS-09	POSITION DESCRIPTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PS-09[01]	security roles and responsibilities are incorporated into organizational position descriptions;
	PS-09[02]	privacy roles and responsibilities are incorporated into organizational position descriptions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PS-09-Examine	[SELECT FROM: Personnel security policy; personnel security procedures; procedures addressing position descriptions; security and privacy position descriptions; system security plan; privacy plan; privacy program plan; other relevant documents or records].
	PS-09-Interview	[SELECT FROM: Organizational personnel with personnel security responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with human capital management responsibilities].
	PS-09-Test	[SELECT FROM: Organizational processes for managing position descriptions].

4.15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY

PT-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-01_ODP[01]	***personnel or roles to whom the personally identifiable information processing and transparency policy is to be disseminated is/are defined;***
	PT-01_ODP[02]	***personnel or roles to whom the personally identifiable information processing and transparency procedures are to be disseminated is/are defined;***
	PT-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	PT-01_ODP[04]	***an official to manage the personally identifiable information processing and transparency policy and procedures is defined;***
	PT-01_ODP[05]	***the frequency at which the current personally identifiable information processing and transparency policy is reviewed and updated is defined;***
	PT-01_ODP[06]	***events that would require the current personally identifiable information processing and transparency policy to be reviewed and updated are defined;***
	PT-01_ODP[07]	***the frequency at which the current personally identifiable information processing and transparency procedures are reviewed and updated is defined;***
	PT-01_ODP[08]	***events that would require the personally identifiable information processing and transparency procedures to be reviewed and updated are defined;***
	PT-01a.[01]	a personally identifiable information processing and transparency policy is developed and documented;
	PT-01a.[02]	the personally identifiable information processing and transparency policy is disseminated to ***<PT-01_ODP[01] personnel or roles>***;
	PT-01a.[03]	personally identifiable information processing and transparency procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and associated personally identifiable information processing and transparency controls are developed and documented;
	PT-01a.[04]	the personally identifiable information processing and transparency procedures are disseminated to ***<PT-01_ODP[02] personnel or roles>***;
	PT-01a.01(a)[01]	the ***<PT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** personally identifiable information processing and transparency policy addresses purpose;
	PT-01a.01(a)[02]	the ***<PT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** personally identifiable information processing and transparency policy addresses scope;
	PT-01a.01(a)[03]	the ***<PT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** personally identifiable information processing and transparency policy addresses roles;
	PT-01a.01(a)[04]	the ***<PT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** personally identifiable information processing and transparency policy addresses responsibilities;
	PT-01a.01(a)[05]	the ***<PT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** personally identifiable information processing and transparency policy addresses management commitment;

PT-01	POLICY AND PROCEDURES	
	PT-01a.01(a)[06]	the ***<PT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** personally identifiable information processing and transparency policy addresses coordination among organizational entities;
	PT-01a.01(a)[07]	the ***<PT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** personally identifiable information processing and transparency policy addresses compliance;
	PT-01a.01(b)	the ***<PT-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** personally identifiable information processing and transparency policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines;
	PT-01b.	the ***<PT-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures;
	PT-01c.01[01]	the current personally identifiable information processing and transparency policy is reviewed and updated ***<PT-01_ODP[05] frequency>***;
	PT-01c.01[02]	the current personally identifiable information processing and transparency policy is reviewed and updated following ***<PT-01_ODP[06] events>***;
	PT-01c.02[01]	the current personally identifiable information processing and transparency procedures are reviewed and updated ***<PT-01_ODP[07] frequency>***;
	PT-01c.02[02]	the current personally identifiable information processing and transparency procedures are reviewed and updated following ***<PT-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-01-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; privacy plan; privacy program plan; other relevant documents or records].
	PT-01-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities].

PT-02	AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-02_ODP[01]	***the authority to permit the processing (defined in PT-02_ODP[02]) of personally identifiable information is defined;***
	PT-02_ODP[02]	***the type of processing of personally identifiable information is defined;***
	PT-02_ODP[03]	***the type of processing of personally identifiable information to be restricted is defined;***
	PT-02a.	the ***<PT-02_ODP[01] authority>*** that permits the ***<PT-02_ODP[02] processing>*** of personally identifiable information is determined and documented;
	PT-02b.	the ***<PT-02_ODP[03] processing>*** of personally identifiable information is restricted to only that which is authorized.

PT-02	AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-02-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; privacy plan; other relevant documents or records].
	PT-02-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-02-Test	[SELECT FROM: Organizational processes for authorizing the processing of personally identifiable information; mechanisms supporting and/or implementing the restriction of personally identifiable information processing].

PT-02(01)	AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION | DATA TAGGING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-02(01)_ODP[01]	***the authorized processing of personally identifiable information is defined;***
	PT-02(01)_ODP[02]	***elements of personally identifiable information to be tagged are defined;***
	PT-02(01)	data tags containing ***<PT-02(01)_ODP[01] authorized processing>*** are attached to ***<PT-02(01)_ODP[02] elements of personally identifiable information>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-02(01)-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures including procedures addressing data tagging; data tag definitions; documented requirements for use and monitoring of data tagging; data extracts with corresponding data tags; privacy plan; other relevant documents or records].
	PT-02(01)-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-02(01)-Test	[SELECT FROM: Organizational processes for authorizing the processing of personally identifiable information; organizational processes for data tagging; mechanisms for applying and monitoring data tagging; mechanisms supporting and/or implementing the restriction of personally identifiable information processing].

PT-02(02)	AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION | AUTOMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-02(02)_ODP	***automated mechanisms used to manage enforcement of the authorized processing of personally identifiable information are defined;***
	PT-02(02)	enforcement of the authorized processing of personally identifiable information is managed using ***<PT-02(02)_ODP automated mechanisms>***.

PT-02(02)	AUTHORITY TO PROCESS PERSONALLY IDENTIFIABLE INFORMATION | AUTOMATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-02(02)-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; privacy plan; other relevant documents or records].
	PT-02(02)-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-02(02)-Test	[SELECT FROM: Organizational processes for authorizing the processing of personally identifiable information; automated mechanisms supporting and/or implementing the management of authorized personally identifiable information processing].

PT-03	PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-03_ODP[01]	***the purpose(s) for processing personally identifiable information is/are defined;***
	PT-03_ODP[02]	***the processing of personally identifiable information to be restricted is defined;***
	PT-03_ODP[03]	***mechanisms to be implemented for ensuring any changes in the processing of personally identifiable information are made in accordance with requirements are defined;***
	PT-03_ODP[04]	***requirements for changing the processing of personally identifiable information are defined;***
	PT-03a.	the ***<PT-03_ODP[01] purpose(s)>*** for processing personally identifiable information is/are identified and documented;
	PT-03b.[01]	the purpose(s) is/are described in the public privacy notices of the organization;
	PT-03b.[02]	the purpose(s) is/are described in the policies of the organization;
	PT-03c.	the ***<PT-03_ODP[02] processing>*** of personally identifiable information are restricted to only that which is compatible with the identified purpose(s);
	PT-03d.[01]	changes in the processing of personally identifiable information are monitored;
	PT-03d.[02]	***<PT-03_ODP[03] mechanisms>*** are implemented to ensure that any changes are made in accordance with ***<PT-03_ODP[04] requirements>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-03-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; configuration management plan; organizational privacy notices; organizational policies; Privacy Act statements; computer matching notices; applicable Federal Register notices; documented requirements for enforcing and monitoring the processing of personally identifiable information; privacy plan; other relevant documents or records].
	PT-03-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities].

PT-03	PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES	
	PT-03-Test	[SELECT FROM: Organizational processes for authorizing the processing of personally identifiable information; mechanisms supporting and/or implementing the management of authorized personally identifiable information processing; organizational processes for monitoring changes in processing personally identifiable information].

PT-03(01)	PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES | DATA TAGGING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-03(01)_ODP[01]	***processing purposes to be contained in data tags are defined;***
	PT-03(01)_ODP[02]	***elements of personally identifiable information to be tagged are defined;***
	PT-03(01)	data tags containing ***<PT-03(01)_ODP[01] processing purposes>*** are attached to ***<PT-03(01)_ODP[02] elements of personally identifiable information>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-03(01)-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; documented description of how data tags are used to identify personally identifiable information data elements and their authorized uses; data tag schema; data extracts with corresponding data tags; privacy plan; other relevant documents or records].
	PT-03(01)-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with data tagging responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-03(01)-Test	[SELECT FROM: Organizational processes for authorizing the processing of personally identifiable information; mechanisms supporting and/or implementing data tagging].

PT-03(02)	PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES | AUTOMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-03(02)_ODP	***automated mechanisms for tracking the processing purposes of personally identifiable information are defined;***
	PT-03(02)	the processing purposes of personally identifiable information are tracked using ***<PT-03(02)_ODP automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-03(02)-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; data extracts with corresponding data tags; privacy plan; other relevant documents or records].

PT-03(02)	PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES | AUTOMATION	
	PT-03(02)-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-03(02)-Test	[SELECT FROM: Organizational processes for managing the enforcement of authorized processing of personally identifiable information; automated tracking mechanisms].

PT-04	CONSENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-04_ODP	***the tools or mechanisms to be implemented for individuals to consent to the processing of their personally identifiable information are defined;***
	PT-04	the ***<PT-04_ODP tools or mechanisms>*** are implemented for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-04-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; consent policies and procedures; consent tools and mechanisms; consent presentation or display (user interface); evidence of individuals' consent; privacy plan; other relevant documents or records].
	PT-04-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-04-Test	[SELECT FROM: Organizational processes for the collection of personally identifiable information; consent tools or mechanisms for users to authorize the processing of their personally identifiable information; mechanisms implementing consent].

PT-04(01)	CONSENT | TAILORED CONSENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-04(01)_ODP	***tailoring mechanisms for processing selected elements of personally identifiable information permissions are defined;***
	PT-04(01)	***<PT-04(01)_ODP mechanisms>*** are provided to allow individuals to tailor processing permissions to selected elements of personally identifiable information.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-04(01)-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; consent policies and procedures; consent tools and mechanisms; consent presentation or display (user interface); privacy plan; other relevant documents or records].

PT-04(01)	CONSENT | TAILORED CONSENT	
	PT-04(01)-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with user interface or user experience responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-04(01)-Test	[SELECT FROM: Organizational processes for consenting to the processing of personally identifiable information; consent tools or mechanisms; mechanisms implementing consent].

PT-04(02)	CONSENT | JUST-IN-TIME CONSENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-04(02)_ODP[01]	***consent mechanisms to be presented to individuals are defined;***
	PT-04(02)_ODP[02]	***the frequency at which to present consent mechanisms to individuals is defined;***
	PT-04(02)_ODP[03]	***personally identifiable information processing to be presented in conjunction with organization-defined consent mechanisms is defined;***
	PT-04(02)	***<PT-04(02)_ODP[01] consent mechanisms>*** are presented to individuals ***<PT-04(02)_ODP[02] frequency>*** and in conjunction with ***<PT-04(02)_ODP[03] personally identifiable information processing>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-04(02)-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; consent policies and procedures; privacy plan; other relevant documents or records].
	PT-04(02)-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with user interface or user experience responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-04(02)-Test	[SELECT FROM: Organizational processes for the collection of personally identifiable information; mechanisms for obtaining just-in-time consent from users for the processing of their personally identifiable information; mechanisms implementing just-in-time consent].

PT-04(03)	CONSENT | REVOCATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-04(03)_ODP	***the tools or mechanisms to be implemented for revoking consent to the processing of personally identifiable information are defined;***
	PT-04(03)	the ***<PT-04(03)_ODP tools or mechanisms>*** are implemented for individuals to revoke consent to the processing of their personally identifiable information.

PT-04(03)	CONSENT | REVOCATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-04(03)-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; consent revocation policies and procedures; consent revocation user interface or user experience; privacy plan; other relevant documents or records].
	PT-04(03)-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with user interface or user experience responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-04(03)-Test	[SELECT FROM: Organizational processes for consenting to the processing of personally identifiable information; tools or mechanisms for implementing consent revocation].

PT-05	PRIVACY NOTICE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-05_ODP[01]	***the frequency at which a notice is provided to individuals after initial interaction with an organization is defined;***
	PT-05_ODP[02]	***information to be included with the notice about the processing of personally identifiable information is defined;***
	PT-05a.[01]	a notice to individuals about the processing of personally identifiable information is provided such that the notice is available to individuals upon first interacting with an organization;
	PT-05a.[02]	a notice to individuals about the processing of personally identifiable information is provided such that the notice is subsequently available to individuals ***<PT-05_ODP[01] frequency>***;
	PT-05b.	a notice to individuals about the processing of personally identifiable information is provided that is clear, easy-to-understand, and expresses information about personally identifiable information processing in plain language;
	PT-05c.	a notice to individuals about the processing of personally identifiable information that identifies the authority that authorizes the processing of personally identifiable information is provided;
	PT-05d.	a notice to individuals about the processing of personally identifiable information that identifies the purpose for which personally identifiable information is to be processed is provided;
	PT-05e.	a notice to individuals about the processing of personally identifiable information which includes ***<PT-05_ODP[02] information>*** is provided.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-05-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; privacy notice; Privacy Act statements; privacy plan; other relevant documents or records].

PT-05	PRIVACY NOTICE	
	PT-05-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with user interface or user experience responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-05-Test	[SELECT FROM: Organizational processes and implementation support or mechanisms for providing notice to individuals regarding the processing of their personally identifiable information].

PT-05(01)	PRIVACY NOTICE | JUST-IN-TIME NOTICE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-05(01)_ODP	***the frequency at which to present a notice of personally identifiable information processing is defined;***
	PT-05(01)	a notice of personally identifiable information processing is presented to individuals at a time and location where the individual provides personally identifiable information, in conjunction with a data action, or ***<PT-05(01)_ODP frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-05(01)-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; privacy notice; privacy plan; other relevant documents or records].
	PT-05(01)-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with user interface or user experience responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-05(01)-Test	[SELECT FROM: Organizational processes and implementation support or mechanisms for providing notice to individuals regarding the processing of their personally identifiable information].

PT-05(02)	PRIVACY NOTICE | PRIVACY ACT STATEMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-05(02)	Privacy Act statements are included on forms that collect information that will be maintained in a Privacy Act system of records, or Privacy Act statements are provided on separate forms that can be retained by individuals.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-05(02)-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; privacy notice; Privacy Act system of records; forms that include Privacy Act statements; privacy plan; other relevant documents or records].

PT-05(02)	PRIVACY NOTICE | PRIVACY ACT STATEMENTS	
	PT-05(02)-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-05(02)-Test	[SELECT FROM: Organizational processes for including Privacy Act statements on forms that collect information or on separate forms that can be retained by individuals].

PT-06	SYSTEM OF RECORDS NOTICE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-06a.[01]	system of records notices are drafted in accordance with OMB guidance for systems that process information that will be maintained in a Privacy Act system of records;
	PT-06a.[02]	new and significantly modified system of records notices are submitted to the OMB and appropriate congressional committees for advance review for systems that process information that will be maintained in a Privacy Act system of records;
	PT-06b.	system of records notices are published in the Federal Register for systems that process information that will be maintained in a Privacy Act system of records;
	PT-06c.	system of records notices are kept accurate, up-to-date, and scoped in accordance with policy for systems that process information that will be maintained in a Privacy Act system of records.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-06-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; privacy notice; Privacy Act system of records; Federal Register notices; privacy plan; other relevant documents or records].
	PT-06-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-06-Test	[SELECT FROM: Organizational processes for Privacy Act system of records maintenance].

PT-06(01)	SYSTEM OF RECORDS NOTICE | ROUTINE USES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-06(01)_ODP	***the frequency at which to review all routine uses published in the system of records notice is defined;***
	PT-06(01)	all routine uses published in the system of records notice are reviewed ***<PT-06(01)_ODP frequency>*** to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.

PT-06(01)	SYSTEM OF RECORDS NOTICE | ROUTINE USES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-06(01)-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; privacy notice; Privacy Act system of records; privacy plan; other relevant documents or records].
	PT-06(01)-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-06(01)-Test	[SELECT FROM: Organizational processes for reviewing system of records notices].

PT-06(02)	SYSTEM OF RECORDS NOTICE | EXEMPTION RULES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-06(02)_ODP	***the frequency at which to review all Privacy Act exemptions claimed for the system of records is defined;***
	PT-06(02)[01]	all Privacy Act exemptions claimed for the system of records are reviewed ***<PT-06(02)_ODP frequency>*** to ensure that they remain appropriate and necessary in accordance with law;
	PT-06(02)[02]	all Privacy Act exemptions claimed for the system of records are reviewed ***<PT-06(02)_ODP frequency>*** to ensure that they have been promulgated as regulations;
	PT-06(02)[03]	all Privacy Act exemptions claimed for the system of records are reviewed ***<PT-06(02)_ODP frequency>*** to ensure that they are accurately described in the system of records notice.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-06(02)-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; privacy notice; Privacy Act system of records; Privacy Act exemptions; privacy plan; other relevant documents or records].
	PT-06(02)-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-06(02)-Test	[SELECT FROM: Organizational processes for Privacy Act system of records maintenance].

PT-07	SPECIFIC CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-07_ODP	***processing conditions to be applied for specific categories of personally identifiable information are defined;***
	PT-07	***<PT-07_ODP processing conditions>*** are applied for specific categories of personally identifiable information.

PT-07	SPECIFIC CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-07-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; privacy notice; Privacy Act system of records; computer matching agreements and notices; contracts; privacy information sharing agreements; memoranda of understanding; governing requirements; privacy plan; other relevant documents or records].
	PT-07-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-07-Test	[SELECT FROM: Organizational processes for supporting and/or implementing personally identifiable information processing].

PT-07(01)	SPECIFIC CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION | SOCIAL SECURITY NUMBERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-07(01)(a)[01]	when a system processes Social Security numbers, the unnecessary collection, maintenance, and use of Social Security numbers are eliminated;
	PT-07(01)(a)[02]	when a system processes Social Security numbers, alternatives to the use of Social Security Numbers as a personal identifier are explored;
	PT-07(01)(b)	when a system processes Social Security numbers, individual rights, benefits, or privileges provided by law are not denied because of an individual's refusal to disclose their Social Security number;
	PT-07(01)(c)[01]	when a system processes Social Security numbers, any individual who is asked to disclose their Social Security number is informed whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it;
	PT-07(01)(c)[02]	when a system processes Social Security numbers, any individual who is asked to disclose their Social Security number is informed by what statutory or other authority the number is solicited;
	PT-07(01)(c)[03]	when a system processes Social Security numbers, any individual who is asked to disclose their Social Security number is informed what uses will be made of it.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-07(01)-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; privacy notice; Privacy Act system of records; privacy notice; separate notice regarding the use of Social Security numbers; privacy plan; other relevant documents or records].
	PT-07(01)-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-07(01)-Test	[SELECT FROM: Organizational processes for identifying, reviewing, and taking action to control the unnecessary use of Social Security numbers; implementation of an alternative to Social Security numbers as identifiers].

PT-07(02)	SPECIFIC CATEGORIES OF PERSONALLY IDENTIFIABLE INFORMATION | FIRST AMENDMENT INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-07(02)	the processing of information describing how any individual exercises rights guaranteed by the First Amendment is prohibited unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-07(02)-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; privacy notice; Privacy Act system of records; privacy plan; other relevant documents or records].
	PT-07(02)-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-07(02)-Test	[SELECT FROM: Organizational processes for supporting and/or implementing personally identifiable information processing].

PT-08	COMPUTER MATCHING REQUIREMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-08a.	approval to conduct the matching program is obtained from the Data Integrity Board when a system or organization processes information for the purpose of conducting a matching program;
	PT-08b.[01]	a computer matching agreement is developed when a system or organization processes information for the purpose of conducting a matching program;
	PT-08b.[02]	a computer matching agreement is entered into when a system or organization processes information for the purpose of conducting a matching program;
	PT-08c.	a matching notice is published in the Federal Register when a system or organization processes information for the purpose of conducting a matching program;
	PT-08d.	the information produced by the matching program is independently verified before taking adverse action against an individual, if required, when a system or organization processes information for the purpose of conducting a matching program;
	PT-08e.[01]	individuals are provided with notice when a system or organization processes information for the purpose of conducting a matching program;
	PT-08e.[02]	individuals are provided with an opportunity to contest the findings before adverse action is taken against them when a system or organization processes information for the purpose of conducting a matching program.

PT-08	COMPUTER MATCHING REQUIREMENTS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-08-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; privacy notice; Privacy Act system of records; Federal Register notices; Data Integrity Board determinations; contracts; information sharing agreements; memoranda of understanding; governing requirements; privacy plan; other relevant documents or records].
	PT-08-Interview	[SELECT FROM: Organizational personnel with personally identifiable information processing and transparency responsibilities; organizational personnel with information security and privacy responsibilities].
	PT-08-Test	[SELECT FROM: Organizational processes for supporting and/or implementing personally identifiable information processing; matching program].

4.16 RISK ASSESSMENT

RA-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-01_ODP[01]	***personnel or roles to whom the risk assessment policy is to be disseminated is/are defined;***
	RA-01_ODP[02]	***personnel or roles to whom the risk assessment procedures are to be disseminated is/are defined;***
	RA-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	RA-01_ODP[04]	***an official to manage the risk assessment policy and procedures is defined;***
	RA-01_ODP[05]	***the frequency at which the current risk assessment policy is reviewed and updated is defined;***
	RA-01_ODP[06]	***events that would require the current risk assessment policy to be reviewed and updated are defined;***
	RA-01_ODP[07]	***the frequency at which the current risk assessment procedures are reviewed and updated is defined;***
	RA-01_ODP[08]	***events that would require risk assessment procedures to be reviewed and updated are defined;***
	RA-01a.[01]	a risk assessment policy is developed and documented;
	RA-01a.[02]	the risk assessment policy is disseminated to ***<RA-01_ODP[01] personnel or roles>***;
	RA-01a.[03]	risk assessment procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls are developed and documented;
	RA-01a.[04]	the risk assessment procedures are disseminated to ***<RA-01_ODP[02] personnel or roles>***;
	RA-01a.01(a)[01]	the ***<RA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** risk assessment policy addresses purpose;
	RA-01a.01(a)[02]	the ***<RA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** risk assessment policy addresses scope;
	RA-01a.01(a)[03]	the ***<RA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** risk assessment policy addresses roles;
	RA-01a.01(a)[04]	the ***<RA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** risk assessment policy addresses responsibilities;
	RA-01a.01(a)[05]	the ***<RA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** risk assessment policy addresses management commitment;
	RA-01a.01(a)[06]	the ***<RA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** risk assessment policy addresses coordination among organizational entities;
	RA-01a.01(a)[07]	the ***<RA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** risk assessment policy addresses compliance;

RA-01	POLICY AND PROCEDURES	
	RA-01a.01(b)	the ***<RA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** risk assessment policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines;
	RA-01b.	the ***<RA-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the risk assessment policy and procedures;
	RA-01c.01[01]	the current risk assessment policy is reviewed and updated ***<RA-01_ODP[05] frequency>***;
	RA-01c.01[02]	the current risk assessment policy is reviewed and updated following ***<RA-01_ODP[06] events>***;
	RA-01c.02[01]	the current risk assessment procedures are reviewed and updated ***<RA-01_ODP[07] frequency>***;
	RA-01c.02[02]	the current risk assessment procedures are reviewed and updated following ***<RA-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-01-Examine	[SELECT FROM: Risk assessment policy and procedures; system security plan; privacy plan; other relevant documents or records].
	RA-01-Interview	[SELECT FROM: Organizational personnel with risk assessment responsibilities; organizational personnel with security and privacy responsibilities].

RA-02	SECURITY CATEGORIZATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-02a.	the system and the information it processes, stores, and transmits are categorized;
	RA-02b.	the security categorization results, including supporting rationale, are documented in the security plan for the system;
	RA-02c.	the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-02-Examine	[SELECT FROM: Risk assessment policy; security planning policy and procedures; procedures addressing security categorization of organizational information and systems; security categorization documentation; system security plan; privacy plan; other relevant documents or records].
	RA-02-Interview	[SELECT FROM: Organizational personnel with security categorization and risk assessment responsibilities; organizational personnel with security and privacy responsibilities].
	RA-02-Test	[SELECT FROM: Organizational processes for security categorization].

RA-02(01)	SECURITY CATEGORIZATION | IMPACT-LEVEL PRIORITIZATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-02(01)	an impact-level prioritization of organizational systems is conducted to obtain additional granularity on system impact levels.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-02(01)-Examine	[SELECT FROM: Risk assessment policy; security and privacy planning policy and procedures; procedures addressing security categorization of organizational information and systems; security categorization documentation; system security plan; privacy plan; other relevant documents or records].
	RA-02(01)-Interview	[SELECT FROM: Organizational personnel with security categorization and risk assessment responsibilities; organizational personnel with security and privacy responsibilities].
	RA-02(01)-Test	[SELECT FROM: Organizational processes for security categorization].

RA-03	RISK ASSESSMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-03_ODP[01]	***one of the following PARAMETER VALUES is selected: {security and privacy plans; risk assessment report; <RA-03_ODP[02] document>};***
	RA-03_ODP[02]	***a document in which risk assessment results are to be documented (if not documented in the security and privacy plans or risk assessment report) is defined (if selected);***
	RA-03_ODP[03]	***the frequency to review risk assessment results is defined;***
	RA-03_ODP[04]	***personnel or roles to whom risk assessment results are to be disseminated is/are defined;***
	RA-03_ODP[05]	***the frequency to update the risk assessment is defined;***
	RA-03a.01	a risk assessment is conducted to identify threats to and vulnerabilities in the system;
	RA-03a.02	a risk assessment is conducted to determine the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system; the information it processes, stores, or transmits; and any related information;
	RA-03a.03	a risk assessment is conducted to determine the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;
	RA-03b.	risk assessment results and risk management decisions from the organization and mission or business process perspectives are integrated with system-level risk assessments;
	RA-03c.	risk assessment results are documented in ***<RA-03_ODP[01] SELECTED PARAMETER VALUE>***;
	RA-03d.	risk assessment results are reviewed ***<RA-03_ODP[03] frequency>***;

RA-03	RISK ASSESSMENT	
	RA-03e.	risk assessment results are disseminated to ***<RA-03_ODP[04] personnel or roles>***;
	RA-03f.	the risk assessment is updated ***<RA-03_ODP[05] frequency>*** or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-03-Examine	[SELECT FROM: Risk assessment policy; risk assessment procedures; security and privacy planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; system security plan; privacy plan; other relevant documents or records].
	RA-03-Interview	[SELECT FROM: Organizational personnel with risk assessment responsibilities; organizational personnel with security and privacy responsibilities].
	RA-03-Test	[SELECT FROM: Organizational processes for risk assessment; mechanisms supporting and/or conducting, documenting, reviewing, disseminating, and updating the risk assessment].

RA-03(01)	RISK ASSESSMENT | SUPPLY CHAIN RISK ASSESSMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-03(01)_ODP[01]	***systems, system components, and system services to assess supply chain risks are defined;***
	RA-03(01)_ODP[02]	***the frequency at which to update the supply chain risk assessment is defined;***
	RA-03(01)(a)	supply chain risks associated with ***<RA-03(01)_ODP[01] systems, system components, and system services>*** are assessed;
	RA-03(01)(b)	the supply chain risk assessment is updated ***<RA-03(01)_ODP[02] frequency>*** , when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-03(01)-Examine	[SELECT FROM: Supply chain risk management policy; inventory of critical systems, system components, and system services; risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of supply chain risk; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; acquisition policy; system security plan; supply chain risk management plan; other relevant documents or records].
	RA-03(01)-Interview	[SELECT FROM: Organizational personnel with risk assessment responsibilities; organizational personnel with security responsibilities; organizational personnel with supply chain risk management responsibilities].
	RA-03(01)-Test	[SELECT FROM: Organizational processes for risk assessment; mechanisms supporting and/or conducting, documenting, reviewing, disseminating, and updating the supply chain risk assessment].

RA-03(02)	RISK ASSESSMENT | USE OF ALL-SOURCE INTELLIGENCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-03(02)	all-source intelligence is used to assist in the analysis of risk.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-03(02)-Examine	[SELECT FROM: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; risk intelligence reports; system security plan; other relevant documents or records].
	RA-03(02)-Interview	[SELECT FROM: Organizational personnel with risk assessment responsibilities; organizational personnel with security responsibilities].
	RA-03(02)-Test	[SELECT FROM: Organizational processes for risk assessment; mechanisms supporting and/or conducting, documenting, reviewing, disseminating, and updating the risk assessment].

RA-03(03)	RISK ASSESSMENT | DYNAMIC THREAT AWARENESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-03(03)_ODP	***means to determine the current cyber threat environment on an ongoing basis;***
	RA-03(03)	the current cyber threat environment is determined on an ongoing basis using ***<RA-03(03)_ODP means>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-03(03)-Examine	[SELECT FROM: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; risk reports; system security plan; other relevant documents or records].
	RA-03(03)-Interview	[SELECT FROM: Organizational personnel with risk assessment responsibilities; organizational personnel with security responsibilities].
	RA-03(03)-Test	[SELECT FROM: Organizational processes for risk assessment; mechanisms supporting and/or conducting, documenting, reviewing, disseminating, and updating the risk assessment].

RA-03(04)	RISK ASSESSMENT | PREDICTIVE CYBER ANALYTICS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-03(04)_ODP[01]	***advanced automation capabilities to predict and identify risks are defined;***
	RA-03(04)_ODP[02]	***systems or system components where advanced automation and analytics capabilities are to be employed are defined;***
	RA-03(04)_ODP[03]	***advanced analytics capabilities to predict and identify risks are defined;***

RA-03(04)	RISK ASSESSMENT | PREDICTIVE CYBER ANALYTICS	
	RA-03(04)[01]	***<RA-03(04)_ODP[01] advanced automation capabilities>*** are employed to predict and identify risks to ***<RA-03(04)_ODP[02] systems or system components>***;
	RA-03(04)[02]	***<RA-03(04)_ODP[03] advanced analytics capabilities>*** are employed to predict and identify risks to ***<RA-03(04)_ODP[02] systems or system components>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-03(04)-Examine	[SELECT FROM: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; risk reports; system security plan; other relevant documents or records].
	RA-03(04)-Interview	[SELECT FROM: Organizational personnel with risk assessment responsibilities; organizational personnel with security responsibilities].
	RA-03(04)-Test	[SELECT FROM: Organizational processes for risk assessment; mechanisms supporting and/or conducting, documenting, reviewing, disseminating, and updating the risk assessment].

RA-04	RISK ASSESSMENT UPDATE
	[WITHDRAWN: Incorporated into RA-03.]

RA-05	VULNERABILITY MONITORING AND SCANNING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-05_ODP[01]	***frequency for monitoring systems and hosted applications for vulnerabilities is defined;***
	RA-05_ODP[02]	***frequency for scanning systems and hosted applications for vulnerabilities is defined;***
	RA-05_ODP[03]	***response times to remediate legitimate vulnerabilities in accordance with an organizational assessment of risk are defined;***
	RA-05_ODP[04]	***personnel or roles with whom information obtained from the vulnerability scanning process and control assessments is to be shared;***
	RA-05a.[01]	systems and hosted applications are monitored for vulnerabilities ***<RA-05_ODP[01] frequency and/or randomly in accordance with organization-defined process>*** and when new vulnerabilities potentially affecting the system are identified and reported;
	RA-05a.[02]	systems and hosted applications are scanned for vulnerabilities ***<RA-05_ODP[02] frequency and/or randomly in accordance with organization-defined process>*** and when new vulnerabilities potentially affecting the system are identified and reported;
	RA-05b.	vulnerability monitoring tools and techniques are employed to facilitate interoperability among tools;

RA-05	VULNERABILITY MONITORING AND SCANNING	
	RA-05b.01	vulnerability monitoring tools and techniques are employed to automate parts of the vulnerability management process by using standards for enumerating platforms, software flaws, and improper configurations;
	RA-05b.02	vulnerability monitoring tools and techniques are employed to facilitate interoperability among tools and to automate parts of the vulnerability management process by using standards for formatting checklists and test procedures;
	RA-05b.03	vulnerability monitoring tools and techniques are employed to facilitate interoperability among tools and to automate parts of the vulnerability management process by using standards for measuring vulnerability impact;
	RA-05c.	vulnerability scan reports and results from vulnerability monitoring are analyzed;
	RA-05d.	legitimate vulnerabilities are remediated ***<RA-05_ODP[03] response times>*** in accordance with an organizational assessment of risk;
	RA-05e.	information obtained from the vulnerability monitoring process and control assessments is shared with ***<RA-05_ODP[04] personnel or roles>*** to help eliminate similar vulnerabilities in other systems;
	RA-05f.	vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned are employed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-05-Examine	[SELECT FROM: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; system security plan; other relevant documents or records].
	RA-05-Interview	[SELECT FROM: Organizational personnel with risk assessment, control assessment, and vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel with vulnerability remediation responsibilities; organizational personnel with security responsibilities; system/network administrators].
	RA-05-Test	[SELECT FROM: Organizational processes for vulnerability scanning, analysis, remediation, and information sharing; mechanisms supporting and/or implementing vulnerability scanning, analysis, remediation, and information sharing].

RA-05(01)	VULNERABILITY MONITORING AND SCANNING | UPDATE TOOL CAPABILITY
	[WITHDRAWN: Incorporated into RA-05.]

RA-05(02)	VULNERABILITY MONITORING AND SCANNING | UPDATE VULNERABILITIES TO BE SCANNED	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-05(02)_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {<RA-05(02)_ODP[02] frequency>; prior to a new scan; when new vulnerabilities are identified and reported};***
	RA-05(02)_ODP[02]	***the frequency for updating the system vulnerabilities to be scanned is defined (if selected);***
	RA-05(02)	the system vulnerabilities to be scanned are updated ***<RA-05(02)_ODP[01] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-05(02)-Examine	[SELECT FROM: Procedures addressing vulnerability scanning; assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; system security plan; other relevant documents or records].
	RA-05(02)-Interview	[SELECT FROM: Organizational personnel with vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel with security responsibilities; system/ network administrators].
	RA-05(02)-Test	[SELECT FROM: Organizational processes for vulnerability scanning; mechanisms/ tools supporting and/or implementing vulnerability scanning].

RA-05(03)	VULNERABILITY MONITORING AND SCANNING | BREADTH AND DEPTH OF COVERAGE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-05(03)	the breadth and depth of vulnerability scanning coverage are defined.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-05(03)-Examine	[SELECT FROM: Procedures addressing vulnerability scanning; assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; system security plan; other relevant documents or records].
	RA-05(03)-Interview	[SELECT FROM: Organizational personnel with vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel with security responsibilities].
	RA-05(03)-Test	[SELECT FROM: Organizational processes for vulnerability scanning; mechanisms/ tools supporting and/or implementing vulnerability scanning].

RA-05(04)	VULNERABILITY MONITORING AND SCANNING | DISCOVERABLE INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-05(04)_ODP	***corrective actions to be taken if information about the system is discoverable are defined;***
	RA-05(04)[01]	information about the system is discoverable;
	RA-05(04)[02]	***<RA-05(04)_ODP corrective actions>*** are taken when information about the system is confirmed as discoverable.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-05(04)-Examine	[SELECT FROM: Procedures addressing vulnerability scanning; assessment report; penetration test results; vulnerability scanning results; risk assessment report; records of corrective actions taken; incident response records; audit records; system security plan; other relevant documents or records].
	RA-05(04)-Interview	[SELECT FROM: Organizational personnel with vulnerability scanning and/or penetration testing responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel responsible for risk response; organizational personnel responsible for incident management and response; organizational personnel with security responsibilities].
	RA-05(04)-Test	[SELECT FROM: Organizational processes for vulnerability scanning; organizational processes for risk response; organizational processes for incident management and response; mechanisms/tools supporting and/or implementing vulnerability scanning; mechanisms supporting and/or implementing risk response; mechanisms supporting and/or implementing incident management and response].

RA-05(05)	VULNERABILITY MONITORING AND SCANNING | PRIVILEGED ACCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-05(05)_ODP[01]	***system components to which privileged access is authorized for selected vulnerability scanning activities are defined;***
	RA-05(05)_ODP[02]	***vulnerability scanning activities selected for privileged access authorization to system components are defined;***
	RA-05(05)	privileged access authorization is implemented to ***<RA-05(05)_ODP[01] system components>*** for ***<RA-05(05)_ODP[02] vulnerability scanning activities>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-05(05)-Examine	[SELECT FROM: Risk assessment policy; procedures addressing vulnerability scanning; system design documentation; system configuration settings and associated documentation; list of system components for vulnerability scanning; personnel access authorization list; authorization credentials; access authorization records; system security plan; other relevant documents or records].
	RA-05(05)-Interview	[SELECT FROM: Organizational personnel with vulnerability scanning responsibilities; system/network administrators; organizational personnel responsible for access control to the system; organizational personnel responsible for configuration management of the system; system developers; organizational personnel with security responsibilities].

RA-05(05)	VULNERABILITY MONITORING AND SCANNING | PRIVILEGED ACCESS	
	RA-05(05)-Test	[SELECT FROM: Organizational processes for vulnerability scanning; organizational processes for access control; mechanisms supporting and/or implementing access control; mechanisms/tools supporting and/or implementing vulnerability scanning].

RA-05(06)	VULNERABILITY MONITORING AND SCANNING | AUTOMATED TREND ANALYSES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-05(06)_ODP	***automated mechanisms to compare the results of multiple vulnerability scans are defined;***
	RA-05(06)	the results of multiple vulnerability scans are compared using ***<RA-05(06)_ODP automated mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-05(06)-Examine	[SELECT FROM: Risk assessment policy; procedures addressing vulnerability scanning; system design documentation; vulnerability scanning tools and techniques documentation; vulnerability scanning results; system security plan; other relevant documents or records].
	RA-05(06)-Interview	[SELECT FROM: Organizational personnel with vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel with security responsibilities].
	RA-05(06)-Test	[SELECT FROM: Organizational processes for vulnerability scanning; automated mechanisms/tools supporting and/or implementing vulnerability scanning; automated mechanisms supporting and/or implementing trend analysis of vulnerability scan results].

RA-05(07)	VULNERABILITY MONITORING AND SCANNING | AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS	
	[WITHDRAWN: Incorporated into CM-08.]	

RA-05(08)	VULNERABILITY MONITORING AND SCANNING | REVIEW HISTORIC AUDIT LOGS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-05(08)_ODP[01]	***a system whose historic audit logs are to be reviewed is defined;***
	RA-05(08)_ODP[02]	***a time period for a potential previous exploit of a system is defined;***
	RA-05(08)	historic audit logs are reviewed to determine if a vulnerability identified in a ***<RA-05(08)_ODP[01] system>*** has been previously exploited within ***<RA-05(08)_ODP[02] time period>***.

RA-05(08)	VULNERABILITY MONITORING AND SCANNING | REVIEW HISTORIC AUDIT LOGS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-05(08)-Examine	[SELECT FROM: Risk assessment policy; procedures addressing vulnerability scanning; audit logs; records of audit log reviews; vulnerability scanning results; patch and vulnerability management records; system security plan; other relevant documents or records].
	RA-05(08)-Interview	[SELECT FROM: Organizational personnel with vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel with audit record review responsibilities; system/network administrators; organizational personnel with security responsibilities].
	RA-05(08)-Test	[SELECT FROM: Organizational processes for vulnerability scanning; organizational process for audit record review and response; mechanisms/tools supporting and/or implementing vulnerability scanning; mechanisms supporting and/or implementing audit record review].

RA-05(09)	VULNERABILITY MONITORING AND SCANNING | PENETRATION TESTING AND ANALYSES	
	[WITHDRAWN: Incorporated into CA-08.]	

RA-05(10)	VULNERABILITY MONITORING AND SCANNING | CORRELATE SCANNING INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-05(10)	the output from vulnerability scanning tools is correlated to determine the presence of multi-vulnerability and multi-hop attack vectors.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-05(10)-Examine	[SELECT FROM: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; vulnerability scanning tools and techniques documentation; vulnerability scanning results; vulnerability management records; audit records; event/vulnerability correlation logs; system security plan; other relevant documents or records].
	RA-05(10)-Interview	[SELECT FROM: Organizational personnel with vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel with security responsibilities].
	RA-05(10)-Test	[SELECT FROM: Organizational processes for vulnerability scanning; mechanisms/tools supporting and/or implementing vulnerability scanning; mechanisms implementing the correlation of vulnerability scan results].

RA-05(11)	VULNERABILITY MONITORING AND SCANNING | PUBLIC DISCLOSURE PROGRAM	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-05(11)	a public reporting channel is established for receiving reports of vulnerabilities in organizational systems and system components.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-05(11)-Examine	[SELECT FROM: Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; vulnerability scanning tools and techniques documentation; vulnerability scanning results; vulnerability management records; audit records; public reporting channel; system security plan; other relevant documents or records].
	RA-05(11)-Interview	[SELECT FROM: Organizational personnel with vulnerability scanning responsibilities; organizational personnel with vulnerability scan analysis responsibilities; organizational personnel with security responsibilities].
	RA-05(11)-Test	[SELECT FROM: Organizational processes for vulnerability scanning; mechanisms/tools supporting and/or implementing vulnerability scanning; mechanisms implementing the public reporting of vulnerabilities].

RA-06	TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-06_ODP[01]	***locations to employ technical surveillance countermeasure surveys are defined;***
	RA-06_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {<RA-06_ODP[03] frequency>; when <RA-06_ODP[04] events or indicators>};***
	RA-06_ODP[03]	***the frequency at which to employ technical surveillance countermeasure surveys is defined (if selected);***
	RA-06_ODP[04]	***events or indicators which, if they occur, trigger a technical surveillance countermeasures survey are defined (if selected);***
	RA-06	a technical surveillance countermeasures survey is employed at ***<RA-06_ODP[01] locations> <RA-06_ODP[02] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-06-Examine	[SELECT FROM: Risk assessment policy; procedures addressing technical surveillance countermeasures surveys; audit records/event logs; system security plan; other relevant documents or records].
	RA-06-Interview	[SELECT FROM: Organizational personnel with technical surveillance countermeasures surveys responsibilities; system/network administrators; organizational personnel with security responsibilities].
	RA-06-Test	[SELECT FROM: Organizational processes for technical surveillance countermeasures surveys; mechanisms/tools supporting and/or implementing technical surveillance countermeasure surveys].

RA-07	RISK RESPONSE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-07[01]	findings from security assessments are responded to in accordance with organizational risk tolerance;
	RA-07[02]	findings from privacy assessments are responded to in accordance with organizational risk tolerance;
	RA-07[03]	findings from monitoring are responded to in accordance with organizational risk tolerance;
	RA-07[04]	findings from audits are responded to in accordance with organizational risk tolerance.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-07-Examine	[SELECT FROM: Risk assessment policy; assessment reports; audit records/event logs; system security plan; privacy plan; other relevant documents or records].
	RA-07-Interview	[SELECT FROM: Organizational personnel with assessment and auditing responsibilities; system/network administrators; organizational personnel with security and privacy responsibilities].
	RA-07-Test	[SELECT FROM: Organizational processes for assessments and audits; mechanisms/tools supporting and/or implementing assessments and auditing].

RA-08	PRIVACY IMPACT ASSESSMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-08a.	privacy impact assessments are conducted for systems, programs, or other activities before developing or procuring information technology that processes personally identifiable information;
	RA-08b.[01]	privacy impact assessments are conducted for systems, programs, or other activities before initiating a collection of personally identifiable information that will be processed using information technology;
	RA-08b.[02]	privacy impact assessments are conducted for systems, programs, or other activities before initiating a collection of personally identifiable information that includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than agencies, instrumentalities, or employees of the federal government.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-08-Examine	[SELECT FROM: Risk assessment policy; security and privacy risk assessment reports; acquisitions documents; system security plan; privacy plan; other relevant documents or records].
	RA-08-Interview	[SELECT FROM: Organizational personnel with assessment and auditing responsibilities; system/network administrators; system developers; program managers; legal counsel; organizational personnel with security and privacy responsibilities].

RA-08	PRIVACY IMPACT ASSESSMENTS	
	RA-08-Test	[SELECT FROM: Organizational processes for assessments and audits; mechanisms/ tools supporting and/or implementing assessments and auditing].

RA-09	CRITICALITY ANALYSIS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-09_ODP[01]	***systems, system components, or system services to be analyzed for criticality are defined;***
	RA-09_ODP[02]	***decision points in the system development life cycle when a criticality analysis is to be performed are defined;***
	RA-09	critical system components and functions are identified by performing a criticality analysis for ***<RA-09_ODP[01] systems, system components, or system services>*** at ***<RA-09_ODP[02] decision points in the system development life cycle>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-09-Examine	[SELECT FROM: Risk assessment policy; assessment reports; criticality analysis/ finalized criticality for each component/subcomponent; audit records/event logs; analysis reports; system security plan; other relevant documents or records].
	RA-09-Interview	[SELECT FROM: Organizational personnel with assessment and auditing responsibilities; organizational personnel with criticality analysis responsibilities; system/network administrators; organizational personnel with security responsibilities].
	RA-09-Test	[SELECT FROM: Organizational processes for assessments and audits; mechanisms/ tools supporting and/or implementing assessments and auditing].

RA-10	THREAT HUNTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	RA-10_ODP	***the frequency at which to employ the threat hunting capability is defined;***
	RA-10a.01	a cyber threat capability is established and maintained to search for indicators of compromise in organizational systems;
	RA-10a.02	a cyber threat capability is established and maintained to detect, track, and disrupt threats that evade existing controls;
	RA-10b.	the threat hunting capability is employed ***<RA-10_ODP frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	RA-10-Examine	[SELECT FROM: Risk assessment policy; assessment reports; audit records/event logs; threat hunting capability; system security plan; other relevant documents or records].

RA-10	THREAT HUNTING	
	RA-10-Interview	[SELECT FROM: Organizational personnel with threat hunting responsibilities; system/network administrators; organizational personnel with security responsibilities].
	RA-10-Test	[SELECT FROM: Organizational processes for assessments and audits; mechanisms/ tools supporting and/or implementing threat hunting capabilities].

4.17 SYSTEM AND SERVICES ACQUISITION

SA-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-01_ODP[01]	***personnel or roles to whom the system and services acquisition policy is to be disseminated is/are defined;***
	SA-01_ODP[02]	***personnel or roles to whom the system and services acquisition procedures are to be disseminated is/are defined;***
	SA-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	SA-01_ODP[04]	***an official to manage the system and services acquisition policy and procedures is defined;***
	SA-01_ODP[05]	***the frequency at which the current system and services acquisition policy is reviewed and updated is defined;***
	SA-01_ODP[06]	***events that would require the current system and services acquisition policy to be reviewed and updated are defined;***
	SA-01_ODP[07]	***the frequency at which the current system and services acquisition procedures are reviewed and updated is defined;***
	SA-01_ODP[08]	***events that would require the system and services acquisition procedures to be reviewed and updated are defined;***
	SA-01a.[01]	a system and services acquisition policy is developed and documented;
	SA-01a.[02]	the system and services acquisition policy is disseminated to ***<SA-01_ODP[01] personnel or roles>***;
	SA-01a.[03]	system and services acquisition procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls are developed and documented;
	SA-01a.[04]	the system and services acquisition procedures are disseminated to ***<SA-01_ODP[02] personnel or roles>***;
	SA-01a.01(a)[01]	the ***<SA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and services acquisition policy addresses purpose;
	SA-01a.01(a)[02]	the ***<SA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and services acquisition policy addresses scope;
	SA-01a.01(a)[03]	the ***<SA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and services acquisition policy addresses roles;
	SA-01a.01(a)[04]	the ***<SA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and services acquisition policy addresses responsibilities;
	SA-01a.01(a)[05]	the ***<SA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and services acquisition policy addresses management commitment;
	SA-01a.01(a)[06]	the ***<SA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and services acquisition policy addresses coordination among organizational entities;

SA-01	POLICY AND PROCEDURES	
	SA-01a.01(a)[07]	the ***<SA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and services acquisition policy addresses compliance;
	SA-01a.01(b)	the ***<SA-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and services acquisition policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines;
	SA-01b.	the ***<SA-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures;
	SA-01c.01[01]	the system and services acquisition policy is reviewed and updated ***<SA-01_ODP[05] frequency>***;
	SA-01c.01[02]	the current system and services acquisition policy is reviewed and updated following ***<SA-01_ODP[06] events>***;
	SA-01c.02[01]	the current system and services acquisition procedures are reviewed and updated ***<SA-01_ODP[07] frequency>***;
	SA-01c.02[02]	the current system and services acquisition procedures are reviewed and updated following ***<SA-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-01-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; supply chain risk management policy; supply chain risk management procedures; supply chain risk management plan; system security plan; privacy plan; other relevant documents or records].
	SA-01-Interview	[SELECT FROM: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities].

SA-02	ALLOCATION OF RESOURCES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-02a.[01]	the high-level information security requirements for the system or system service are determined in mission and business process planning;
	SA-02a.[02]	the high-level privacy requirements for the system or system service are determined in mission and business process planning;
	SA-02b.[01]	the resources required to protect the system or system service are determined and documented as part of the organizational capital planning and investment control process;
	SA-02b.[02]	the resources required to protect the system or system service are allocated as part of the organizational capital planning and investment control process;
	SA-02c.[01]	a discrete line item for information security is established in organizational programming and budgeting documentation;
	SA-02c.[02]	a discrete line item for privacy is established in organizational programming and budgeting documentation.

SA-02	ALLOCATION OF RESOURCES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-02-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; system and services acquisition strategy and plans; procedures addressing the allocation of resources to information security and privacy requirements; procedures addressing capital planning and investment control; organizational programming and budgeting documentation; system security plan; privacy plan; supply chain risk management policy; other relevant documents or records].
	SA-02-Interview	[SELECT FROM: Organizational personnel with capital planning, investment control, organizational programming, and budgeting responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities].
	SA-02-Test	[SELECT FROM: Organizational processes for determining information security and privacy requirements; organizational processes for capital planning, programming, and budgeting; mechanisms supporting and/or implementing organizational capital planning, programming, and budgeting].

SA-03	SYSTEM DEVELOPMENT LIFE CYCLE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-03_ODP	***system development life cycle is defined;***
	SA-03a.[01]	the system is acquired, developed, and managed using ***<SA-03_ODP system-development life cycle>*** that incorporates information security considerations;
	SA-03a.[02]	the system is acquired, developed, and managed using ***<SA-03_ODP system-development life cycle>*** that incorporates privacy considerations;
	SA-03b.[01]	information security roles and responsibilities are defined and documented throughout the system development life cycle;
	SA-03b.[02]	privacy roles and responsibilities are defined and documented throughout the system development life cycle;
	SA-03c.[01]	individuals with information security roles and responsibilities are identified;
	SA-03c.[02]	individuals with privacy roles and responsibilities are identified;
	SA-03d.[01]	organizational information security risk management processes are integrated into system development life cycle activities;
	SA-03d.[02]	organizational privacy risk management processes are integrated into system development life cycle activities.

SA-03	SYSTEM DEVELOPMENT LIFE CYCLE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-03-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing the integration of information security and privacy and supply chain risk management into the system development life cycle process; system development life cycle documentation; organizational risk management strategy; information security and privacy risk management strategy documentation; system security plan; privacy plan; privacy program plan; enterprise architecture documentation; role-based security and privacy training program documentation; data mapping documentation; other relevant documents or records].
	SA-03-Interview	[SELECT FROM: Organizational personnel with information security and privacy responsibilities; organizational personnel with system life cycle development responsibilities; organizational personnel with supply chain risk management responsibilities].
	SA-03-Test	[SELECT FROM: Organizational processes for defining and documenting the system development life cycle; organizational processes for identifying system development life cycle roles and responsibilities; organizational processes for integrating information security and privacy and supply chain risk management into the system development life cycle; mechanisms supporting and/or implementing the system development life cycle].

SA-03(01)	SYSTEM DEVELOPMENT LIFE CYCLE | MANAGE PREPRODUCTION ENVIRONMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-03(01)	system pre-production environments are protected commensurate with risk throughout the system development life cycle for the system, system component, or system service.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-03(01)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the integration of security and supply chain risk management into the system development life cycle process; system development life cycle documentation; procedures addressing program protection planning; criticality analysis results; security and supply chain risk management strategy/program documentation; system security plan; supply chain risk management plan; other relevant documents or records].
	SA-03(01)-Interview	[SELECT FROM: Organizational personnel with security and system life cycle development responsibilities; organizational personnel with information security responsibilities].
	SA-03(01)-Test	[SELECT FROM: Organizational processes for defining and documenting the system development life cycle; organizational processes for identifying system development life cycle roles and responsibilities; organizational process for integrating security risk management into the system development life cycle; mechanisms supporting and/or implementing the system development life cycle].

SA-03(02)	SYSTEM DEVELOPMENT LIFE CYCLE | USE OF LIVE OR OPERATIONAL DATA	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-03(02)a.[01]	the use of live data in pre-production environments is approved for the system, system component, or system service;
	SA-03(02)a.[02]	the use of live data in pre-production environments is documented for the system, system component, or system service;
	SA-03(02)a.[03]	the use of live data in pre-production environments is controlled for the system, system component, or system service;
	SA-03(02)b.	pre-production environments for the system, system component, or system service are protected at the same impact or classification level as any live data in use within the pre-production environments.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-03(02)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing the integration of security and privacy into the system development life cycle process; system development life cycle documentation; security risk assessment documentation; privacy impact assessment; privacy risk assessment documentation; system security plan; privacy plan; data mapping documentation; personally identifiable information processing policy; procedures addressing the authority to test with personally identifiable information; procedures addressing the minimization of personally identifiable information used in testing, training, and research; other relevant documents or records].
	SA-03(02)-Interview	[SELECT FROM: Organizational personnel with information security and privacy responsibility; organizational personnel with system life cycle development responsibilities].
	SA-03(02)-Test	[SELECT FROM: Organizational processes the use of live data in pre-production environments; mechanisms for protecting live data in pre-production environments].

SA-03(03)	SYSTEM DEVELOPMENT LIFE CYCLE | TECHNOLOGY REFRESH	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-03(03)[01]	a technology refresh schedule is planned for the system throughout the system development life cycle;
	SA-03(03)[02]	a technology refresh schedule is implemented for the system throughout the system development life cycle.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-03(03)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing technology refresh planning and implementation; system development life cycle documentation; technology refresh schedule; security risk assessment documentation; privacy impact assessment; privacy risk assessment documentation; system security plan; privacy plan; other relevant documents or records].

SA-03(03)	SYSTEM DEVELOPMENT LIFE CYCLE | TECHNOLOGY REFRESH	
	SA-03(03)-Interview	[SELECT FROM: Organizational personnel with information security and privacy responsibilities; organizational personnel with system life cycle development responsibilities].
	SA-03(03)-Test	[SELECT FROM: Organizational processes for defining and documenting the system development life cycle; organizational processes for identifying system development life cycle roles and responsibilities; organizational processes for integrating security and privacy risk management into the system development life cycle; mechanisms supporting and/or implementing the system development life cycle].

SA-04	ACQUISITION PROCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-04_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {standardized contract language; <SA-04_ODP[02] contract language>};***
	SA-04_ODP[02]	***contract language is defined (if selected);***
	SA-04a.[01]	security functional requirements, descriptions, and criteria are included explicitly or by reference using ***<SA-04_ODP[01] SELECTED PARAMETER VALUE(S)>*** in the acquisition contract for the system, system component, or system service;
	SA-04a.[02]	privacy functional requirements, descriptions, and criteria are included explicitly or by reference using ***<SA-04_ODP[01] SELECTED PARAMETER VALUE(S)>*** in the acquisition contract for the system, system component, or system service;
	SA-04b.	strength of mechanism requirements, descriptions, and criteria are included explicitly or by reference using ***<SA-04_ODP[01] SELECTED PARAMETER VALUE(S)>*** in the acquisition contract for the system, system component, or system service;
	SA-04c.[01]	security assurance requirements, descriptions, and criteria are included explicitly or by reference using ***<SA-04_ODP[01] SELECTED PARAMETER VALUE(S)>*** in the acquisition contract for the system, system component, or system service;
	SA-04c.[02]	privacy assurance requirements, descriptions, and criteria are included explicitly or by reference using ***<SA-04_ODP[01] SELECTED PARAMETER VALUE(S)>*** in the acquisition contract for the system, system component, or system service;
	SA-04d.[01]	controls needed to satisfy the security requirements, descriptions, and criteria are included explicitly or by reference using ***<SA-04_ODP[01] SELECTED PARAMETER VALUE(S)>*** in the acquisition contract for the system, system component, or system service;
	SA-04d.[02]	controls needed to satisfy the privacy requirements, descriptions, and criteria are included explicitly or by reference using ***<SA-04_ODP[01] SELECTED PARAMETER VALUE(S)>*** in the acquisition contract for the system, system component, or system service;
	SA-04e.[01]	security documentation requirements, descriptions, and criteria are included explicitly or by reference using ***<SA-04_ODP[01] SELECTED PARAMETER VALUE(S)>*** in the acquisition contract for the system, system component, or system service;

SA-04	ACQUISITION PROCESS	
	SA-04e.[02]	privacy documentation requirements, descriptions, and criteria are included explicitly or by reference using ***<SA-04_ODP[01] SELECTED PARAMETER VALUE(S)>*** in the acquisition contract for the system, system component, or system service;
	SA-04f.[01]	requirements for protecting security documentation, descriptions, and criteria are included explicitly or by reference using ***<SA-04_ODP[01] SELECTED PARAMETER VALUE(S)>*** in the acquisition contract for the system, system component, or system service;
	SA-04f.[02]	requirements for protecting privacy documentation, descriptions, and criteria are included explicitly or by reference using ***<SA-04_ODP[01] SELECTED PARAMETER VALUE(S)>*** in the acquisition contract for the system, system component, or system service;
	SA-04g.	the description of the system development environment and environment in which the system is intended to operate, requirements, and criteria are included explicitly or by reference using ***<SA-04_ODP[01] SELECTED PARAMETER VALUE(S)>*** in the acquisition contract for the system, system component, or system service;
	SA-04h.[01]	the allocation of responsibility or identification of parties responsible for information security requirements, descriptions, and criteria are included explicitly or by reference using ***<SA-04_ODP[01] SELECTED PARAMETER VALUE(S)>*** in the acquisition contract for the system, system component, or system service;
	SA-04h.[02]	the allocation of responsibility or identification of parties responsible for privacy requirements, descriptions, and criteria are included explicitly or by reference using ***<SA-04_ODP[01] SELECTED PARAMETER VALUE(S)>***;
	SA-04h.[03]	the allocation of responsibility or identification of parties responsible for supply chain risk management requirements, descriptions, and criteria are included explicitly or by reference using ***<SA-04_ODP[01] SELECTED PARAMETER VALUE(S)>***;
	SA-04i.	acceptance criteria requirements and descriptions are included explicitly or by reference using ***<SA-04_ODP[01] SELECTED PARAMETER VALUE(S)>*** in the acquisition contract for the system, system component, or system service.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-04-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing the integration of information security and privacy and supply chain risk management into the acquisition process; configuration management plan; acquisition contracts for the system, system component, or system service; system design documentation; system security plan; supply chain risk management plan; privacy plan; other relevant documents or records].
	SA-04-Interview	[SELECT FROM: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with information security and privacy responsibilities; system/network administrators; organizational personnel with supply chain risk management responsibilities].
	SA-04-Test	[SELECT FROM: Organizational processes for determining system security and privacy functional, strength, and assurance requirements; organizational processes for developing acquisition contracts; mechanisms supporting and/or implementing acquisitions and the inclusion of security and privacy requirements in contracts].

SA-04(01)	ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF CONTROLS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-04(01)	the developer of the system, system component, or system service is required to provide a description of the functional properties of the controls to be implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-04(01)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing the integration of security and privacy requirements, descriptions, and criteria into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for the system, system component, or system services; system security plan; privacy plan; other relevant documents or records].
	SA-04(01)-Interview	[SELECT FROM: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with information security and privacy responsibilities; system developers].
	SA-04(01)-Test	[SELECT FROM: Organizational processes for determining system security functional requirements; organizational processes for developing acquisition contracts; mechanisms supporting and/or implementing acquisitions and the inclusion of security and privacy requirements in contracts].

SA-04(02)	ACQUISITION PROCESS | DESIGN AND IMPLEMENTATION INFORMATION FOR CONTROLS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-04(02)_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; <SA-04(02)_ODP[02] design and implementation information>};***
	SA-04(02)_ODP[02]	***design and implementation information is defined (if selected);***
	SA-04(02)_ODP[03]	***level of detail is defined;***
	SA-04(02)	the developer of the system, system component, or system service is required to provide design and implementation information for the controls that includes using ***<SA-04(02)_ODP[01] SELECTED PARAMETER VALUE(S)>*** at ***<SA-04(02)_ODP[03] level of detail>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-04(02)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing the integration of security requirements, descriptions, and criteria into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for the system, system components, or system services; design and implementation information for controls employed in the system, system component, or system service; system security plan; other relevant documents or records].

SA-04(02)	ACQUISITION PROCESS | DESIGN AND IMPLEMENTATION INFORMATION FOR CONTROLS	
	SA-04(02)-Interview	[SELECT FROM: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with the responsibility to determine system security requirements; system developers or service provider; organizational personnel with information security responsibilities].
	SA-04(02)-Test	[SELECT FROM: Organizational processes for determining the level of detail for system design and controls; organizational processes for developing acquisition contracts; mechanisms supporting and/or implementing the development of system design details].

SA-04(03)	ACQUISITION PROCESS | DEVELOPMENT METHODS, TECHNIQUES, AND PRACTICES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-04(03)_ODP[01]	***systems engineering methods are defined;***
	SA-04(03)_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {<SA-04(03)_ODP[03] system security engineering methods>; <SA-04(03)_ODP[04] privacy engineering methods>};***
	SA-04(03)_ODP[03]	***system security engineering methods are defined (if selected);***
	SA-04(03)_ODP[04]	***privacy engineering methods are defined (if selected);***
	SA-04(03)_ODP[05]	***one or more of the following PARAMETER VALUES is/are selected: {<SA-04(03)_ODP[06] software development methods>; <SA-04(03)_ODP[07] testing, evaluation, assessment, verification, and validation methods>; <SA-04(03)_ODP[08] quality control processes>};***
	SA-04(03)_ODP[06]	***software development methods are defined (if selected);***
	SA-04(03)_ODP[07]	***testing, evaluation, assessment, verification, and validation methods are defined (if selected);***
	SA-04(03)_ODP[08]	***quality control processes are defined (if selected);***
	SA-04(03)(a)	the developer of the system, system component, or system service is required to demonstrate the use of a system development life cycle process that includes ***<SA-04(03)_ODP[01] systems engineering methods>***;
	SA-04(03)(b)	the developer of the system, system component, or system service is required to demonstrate the use of a system development life cycle process that includes ***<SA-04(03)_ODP[02] SELECTED PARAMETER VALUE(S)>***;
	SA-04(03)(c)	the developer of the system, system component, or system service is required to demonstrate the use of a system development life cycle process that includes ***<SA-04(03)_ODP[05] SELECTED PARAMETER VALUE(S)>***.

SA-04(03)	ACQUISITION PROCESS | DEVELOPMENT METHODS, TECHNIQUES, AND PRACTICES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-04(03)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing the integration of security and privacy requirements, descriptions, and criteria into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for the system, system component, or system service; list of systems security and privacy engineering methods to be included in the developer's system development life cycle process; list of software development methods to be included in the developer's system development life cycle process; list of testing, evaluation, or validation techniques to be included in the developer's system development life cycle process; list of quality control processes to be included in the developer's system development life cycle process; system security plan; privacy plan; other relevant documents or records].
	SA-04(03)-Interview	[SELECT FROM: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with system life cycle responsibilities; system developers or service provider].
	SA-04(03)-Test	[SELECT FROM: Organizational processes for development methods, techniques, and processes].

SA-04(04)	ACQUISITION PROCESS | ASSIGNMENT OF COMPONENTS TO SYSTEMS
	[WITHDRAWN: Incorporated into CM-08(09).]

SA-04(05)	ACQUISITION PROCESS | SYSTEM, COMPONENT, AND SERVICE CONFIGURATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-04(05)_ODP	***security configurations for the system, component, or service are defined;***
	SA-04(05)(a)	the developer of the system, system component, or system service is required to deliver the system, component, or service with ***<SA-04(05)_ODP security configurations>*** implemented;
	SA-04(05)(b)	the configurations are used as the default for any subsequent system, component, or service reinstallation or upgrade.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-04(05)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the integration of security requirements, descriptions, and criteria into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for the system, system component, or system service; security configurations to be implemented by the developer of the system, system component, or system service; service level agreements; system security plan; other relevant documents or records].

SA-04(05)	ACQUISITION PROCESS | SYSTEM, COMPONENT, AND SERVICE CONFIGURATIONS	
	SA-04(05)-Interview	[SELECT FROM: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with the responsibility to determine system security requirements; system developers or service provider; organizational personnel with information security responsibilities].
	SA-04(05)-Test	[SELECT FROM: Mechanisms used to verify that the configuration of the system, component, or service is delivered as specified].

SA-04(06)	ACQUISITION PROCESS | USE OF INFORMATION ASSURANCE PRODUCTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-04(06)(a)	only government off-the-shelf or commercial off-the-shelf information assurance and information assurance-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted are employed;
	SA-04(06)(b)	these products have been evaluated and/or validated by NSA or in accordance with NSA-approved procedures.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-04(06)-Examine	[SELECT FROM: Supply chain risk management plan; system and services acquisition policy; procedures addressing the integration of security requirements, descriptions, and criteria into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for the system, system component, or system service; security configurations to be implemented by the developer of the system, system component, or system service; service level agreements; list of deployed IT products/solutions; NSA-approved list; system security plan; other relevant documents or records].
	SA-04(06)-Interview	[SELECT FROM: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with the responsibility to determine system security requirements; organizational personnel responsible for ensuring information assurance products are NSA-approved and are evaluated and/or validated products in accordance with NSA-approved procedures; organizational personnel with information security responsibilities].
	SA-04(06)-Test	[SELECT FROM: Organizational processes for selecting and employing evaluated and/or validated information assurance products and services that compose an NSA-approved solution to protect classified information].

SA-04(07)	ACQUISITION PROCESS | NIAP-APPROVED PROTECTION PROFILES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-04(07)(a)	the use of commercially provided information assurance and information assurance-enabled information technology products is limited to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists;
	SA-04(07)(b)	if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that cryptographic module is required to be FIPS-validated or NSA-approved.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-04(07)-Examine	[SELECT FROM: Supply chain risk management plan; system and services acquisition policy; procedures addressing the integration of security requirements, descriptions, and criteria into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for the system, system component, or system service; list of deployed IT products/solutions; NAIP-approved protection profiles; FIPS-validation information for cryptographic functionality; system security plan; other relevant documents or records].
	SA-04(07)-Interview	[SELECT FROM: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with the responsibility for determining system security requirements; organizational personnel responsible for ensuring that information assurance products have been evaluated against a NIAP-approved protection profile or for ensuring products relying on cryptographic functionality are FIPS-validated; organizational personnel with information security responsibilities].
	SA-04(07)-Test	[SELECT FROM: Organizational processes for selecting and employing products/services evaluated against a NIAP-approved protection profile or FIPS-validated products].

SA-04(08)	ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN FOR CONTROLS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-04(08)	the developer of the system, system component, or system service is required to produce a plan for the continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the organization.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-04(08)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing developer continuous monitoring plans; procedures addressing the integration of security requirements, descriptions, and criteria into the acquisition process; developer continuous monitoring plans; security assessment plans; acquisition contracts for the system, system component, or system service; acquisition documentation; solicitation documentation; service level agreements; system security plan; other relevant documents or records].

SA-04(08)	ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN FOR CONTROLS	
	SA-04(08)-Interview	[SELECT FROM: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with the responsibility for determining system security requirements; system developers; organizational personnel with information security responsibilities].
	SA-04(08)-Test	[SELECT FROM: Vendor processes for continuous monitoring; mechanisms supporting and/or implementing developer continuous monitoring].

SA-04(09)	ACQUISITION PROCESS | FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES IN USE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-04(09)[01]	the developer of the system, system component, or system service is required to identify the functions intended for organizational use;
	SA-04(09)[02]	the developer of the system, system component, or system service is required to identify the ports intended for organizational use;
	SA-04(09)[03]	the developer of the system, system component, or system service is required to identify the protocols intended for organizational use;
	SA-04(09)[04]	the developer of the system, system component, or system service is required to identify the services intended for organizational use.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-04(09)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the integration of security requirements, descriptions, and criteria into the acquisition process; system design documentation; system documentation, including functions, ports, protocols, and services intended for organizational use; acquisition contracts for systems or services; acquisition documentation; solicitation documentation; service level agreements; organizational security requirements, descriptions, and criteria for developers of systems, system components, and system services; system security plan; other relevant documents or records].
	SA-04(09)-Interview	[SELECT FROM: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with the responsibility for determining system security requirements; system/network administrators; organizational personnel operating, using, and/or maintaining the system; system developers; organizational personnel with information security responsibilities].

SA-04(10)	ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-04(10)	only information technology products on the FIPS 201-approved products list for the Personal Identity Verification (PIV) capability implemented within organizational systems are employed.

SA-04(10)	ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-04(10)-Examine	[SELECT FROM: Supply chain risk management plan; system and services acquisition policy; procedures addressing the integration of security requirements, descriptions, and criteria into the acquisition process; solicitation documentation; acquisition documentation; acquisition contracts for the system, system component, or system service; service level agreements; FIPS 201 approved products list; system security plan; other relevant documents or records].
	SA-04(10)-Interview	[SELECT FROM: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with the responsibility for determining system security requirements; organizational personnel with the responsibility for ensuring that only FIPS 201- approved products are implemented; organizational personnel with information security responsibilities].
	SA-04(10)-Test	[SELECT FROM: Organizational processes for selecting and employing FIPS 201-approved products].

SA-04(11)	ACQUISITION PROCESS | SYSTEM OF RECORDS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-04(11)_ODP	***Privacy Act requirements for the operation of a system of records are defined;***
	SA-04(11)	***<SA-04(11)_ODP Privacy Act requirements>*** are defined in the acquisition contract for the operation of a system of records on behalf of an organization to accomplish an organizational mission or function.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-04(11)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing the integration of Privacy Act requirements into systems of records operated by external organizations; solicitation documentation; acquisition documentation; acquisition contracts for the system, system component, or system service; service level agreements; system security plan; privacy plan; personally identifiable information processing policy; privacy program plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SA-04(11)-Interview	[SELECT FROM: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities].
	SA-04(11)-Test	[SELECT FROM: Contract management processes to verify Privacy Act requirements are defined for the operation of a system of records; vendor processes for demonstrating incorporation of Privacy Act requirements in its operation of a system of records].

SA-04(12)	ACQUISITION PROCESS | DATA OWNERSHIP	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-04(12)_ODP	***time frame to remove data from a contractor system and return it to the organization is defined;***
	SA-04(12)(a)	organizational data ownership requirements are included in the acquisition contract;
	SA-04(12)(b)	all data to be removed from the contractor's system and returned to the organization is required within ***<SA-04(12)_ODP time frame>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-04(12)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing the integration of information security and privacy requirements, descriptions, and criteria into the acquisition process; procedures addressing the disposition of personally identifiable information; solicitation documentation; acquisition documentation; acquisition contracts for the system or system service; personally identifiable information processing policy; service level agreements; information sharing agreements; memoranda of understanding; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SA-04(12)-Interview	[SELECT FROM: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with the responsibility for data management and processing requirements; organizational personnel with information security and privacy responsibilities].
	SA-04(12)-Test	[SELECT FROM: Contract management processes to verify that data is removed as required; vendor processes for removing data in required timeframe; mechanisms verifying the removal and return of data].

SA-05	SYSTEM DOCUMENTATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-05_ODP[01]	***actions to take when system, system component, or system service documentation is either unavailable or nonexistent are defined;***
	SA-05_ODP[02]	***personnel or roles to distribute system documentation to is/are defined;***
	SA-05a.01[01]	administrator documentation for the system, system component, or system service that describes the secure configuration of the system, component, or service is obtained or developed;
	SA-05a.01[02]	administrator documentation for the system, system component, or system service that describes the secure installation of the system, component, or service is obtained or developed;
	SA-05a.01[03]	administrator documentation for the system, system component, or system service that describes the secure operation of the system, component, or service is obtained or developed;

SA-05	SYSTEM DOCUMENTATION	
	SA-05a.02[01]	administrator documentation for the system, system component, or system service that describes the effective use of security functions and mechanisms is obtained or developed;
	SA-05a.02[02]	administrator documentation for the system, system component, or system service that describes the effective maintenance of security functions and mechanisms is obtained or developed;
	SA-05a.02[03]	administrator documentation for the system, system component, or system service that describes the effective use of privacy functions and mechanisms is obtained or developed;
	SA-05a.02[04]	administrator documentation for the system, system component, or system service that describes the effective maintenance of privacy functions and mechanisms is obtained or developed;
	SA-05a.03[01]	administrator documentation for the system, system component, or system service that describes known vulnerabilities regarding the configuration of administrative or privileged functions is obtained or developed;
	SA-05a.03[02]	administrator documentation for the system, system component, or system service that describes known vulnerabilities regarding the use of administrative or privileged functions is obtained or developed;
	SA-05b.01[01]	user documentation for the system, system component, or system service that describes user-accessible security functions and mechanisms is obtained or developed;
	SA-05b.01[02]	user documentation for the system, system component, or system service that describes how to effectively use those (user-accessible security) functions and mechanisms is obtained or developed;
	SA-05b.01[03]	user documentation for the system, system component, or system service that describes user-accessible privacy functions and mechanisms is obtained or developed;
	SA-05b.01[04]	user documentation for the system, system component, or system service that describes how to effectively use those (user-accessible privacy) functions and mechanisms is obtained or developed;
	SA-05b.02[01]	user documentation for the system, system component, or system service that describes methods for user interaction, which enable individuals to use the system, component, or service in a more secure manner is obtained or developed;
	SA-05b.02[02]	user documentation for the system, system component, or system service that describes methods for user interaction, which enable individuals to use the system, component, or service to protect individual privacy is obtained or developed;
	SA-05b.03[01]	user documentation for the system, system component, or system service that describes user responsibilities for maintaining the security of the system, component, or service is obtained or developed;
	SA-05b.03[02]	user documentation for the system, system component, or system service that describes user responsibilities for maintaining the privacy of individuals is obtained or developed;
	SA-05c.[01]	attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent is documented;

SA-05	SYSTEM DOCUMENTATION	
	SA-05c.[02]	after attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent, ***<SA-05_ODP[01] actions>*** are taken in response;
	SA-05d.	documentation is distributed to ***<SA-05_ODP[02] personnel or roles>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-05-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing system documentation; system documentation, including administrator and user guides; system design documentation; records documenting attempts to obtain unavailable or nonexistent system documentation; list of actions to be taken in response to documented attempts to obtain system, system component, or system service documentation; risk management strategy documentation; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SA-05-Interview	[SELECT FROM: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with information security and privacy responsibilities; system administrators; organizational personnel responsible for operating, using, and/or maintaining the system; system developers].
	SA-05-Test	[SELECT FROM: Organizational processes for obtaining, protecting, and distributing system administrator and user documentation].

SA-05(01)	SYSTEM DOCUMENTATION | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS
	[WITHDRAWN: Incorporated into SA-04(01).]

SA-05(02)	SYSTEM DOCUMENTATION | SECURITY-RELEVANT EXTERNAL SYSTEM INTERFACES
	[WITHDRAWN: Incorporated into SA-04(02).]

SA-05(03)	SYSTEM DOCUMENTATION | HIGH-LEVEL DESIGN
	[WITHDRAWN: Incorporated into SA-04(02).]

SA-05(04)	SYSTEM DOCUMENTATION | LOW-LEVEL DESIGN
	[WITHDRAWN: Incorporated into SA-04(02).]

SA-05(05)	SYSTEM DOCUMENTATION | SOURCE CODE
	[WITHDRAWN: Incorporated into SA-04(02).]

SA-06	SOFTWARE USAGE RESTRICTIONS
	[WITHDRAWN: Incorporated into CM-10, SI-07.]

SA-07	USER-INSTALLED SOFTWARE
	[WITHDRAWN: Incorporated into CM-11, SI-07.]

SA-08	SECURITY AND PRIVACY ENGINEERING PRINCIPLES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08_ODP[01]	***systems security engineering principles are defined;***
	SA-08_ODP[02]	***privacy engineering principles are defined;***
	SA-08[01]	***<SA-08_ODP[01] systems security engineering principles>*** are applied in the specification of the system and system components;
	SA-08[02]	***<SA-08_ODP[01] systems security engineering principles>*** are applied in the design of the system and system components;
	SA-08[03]	***<SA-08_ODP[01] systems security engineering principles>*** are applied in the development of the system and system components;
	SA-08[04]	***<SA-08_ODP[01] systems security engineering principles>*** are applied in the implementation of the system and system components;
	SA-08[05]	***<SA-08_ODP[01] systems security engineering principles>*** are applied in the modification of the system and system components;
	SA-08[06]	***<SA-08_ODP[02] privacy engineering principles>*** are applied in the specification of the system and system components;
	SA-08[07]	***<SA-08_ODP[02] privacy engineering principles>*** are applied in the design of the system and system components;
	SA-08[08]	***<SA-08_ODP[02] privacy engineering principles>*** are applied in the development of the system and system components;
	SA-08[09]	***<SA-08_ODP[02] privacy engineering principles>*** are applied in the implementation of the system and system components;
	SA-08[10]	***<SA-08_ODP[02] privacy engineering principles>*** are applied in the modification of the system and system components.

SA-08	SECURITY AND PRIVACY ENGINEERING PRINCIPLES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; assessment and authorization procedures; procedures addressing security and privacy engineering principles used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SA-08-Interview	[SELECT FROM: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers].
	SA-08-Test	[SELECT FROM: Organizational processes for applying security and privacy engineering principles in system specification, design, development, implementation, and modification; mechanisms supporting the application of security and privacy engineering principles in system specification, design, development, implementation, and modification].

SA-08(01)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | CLEAR ABSTRACTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(01)	the security design principle of clear abstractions is implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(01)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of clear abstractions used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(01)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(01)-Test	[SELECT FROM: Organizational processes for applying the security design principle of clear abstractions to system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of clear abstractions to system specification, design, development, implementation, and modification].

SA-08(02)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | LEAST COMMON MECHANISM	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(02)_ODP	***systems or system components that implement the security design principle of least common mechanism are defined;***
	SA-08(02)	***<SA-08(02)_ODP systems or system components>*** implement the security design principle of least common mechanism.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(02)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of least common mechanism used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(02)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(02)-Test	[SELECT FROM: Organizational processes for applying the security design principle of least common mechanism in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of least common mechanism in system specification, design, development, implementation, and modification].

SA-08(03)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MODULARITY AND LAYERING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(03)_ODP[01]	***systems or system components that implement the security design principle of modularity are defined;***
	SA-08(03)_ODP[02]	***systems or system components that implement the security design principle of layering are defined;***
	SA-08(03)[01]	***<SA-08(03)_ODP[01] systems or system components>*** implement the security design principle of modularity;
	SA-08(03)[02]	***<SA-08(03)_ODP[02] systems or system components>*** implement the security design principle of layering.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(03)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principles of modularity and layering used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].

SA-08(03)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MODULARITY AND LAYERING	
	SA-08(03)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(03)-Test	[SELECT FROM: Organizational processes for applying the security design principles of modularity and layering in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principles of modularity and layering in system specification, design, development, implementation, and modification; mechanisms supporting and/or implementing an isolation boundary].

SA-08(04)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | PARTIALLY ORDERED DEPENDENCIES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(04)_ODP	***systems or system components that implement the security design principle of partially ordered dependencies are defined;***
	SA-08(04)	***<SA-08(04)_ODP systems or system components>*** implement the security design principle of partially ordered dependencies.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(04)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of partially ordered dependencies used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(04)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(04)-Test	[SELECT FROM: Organizational processes for applying the security design principle of partially ordered dependencies in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of partially ordered dependencies in system specification, design, development, implementation, and modification].

SA-08(05)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | EFFICIENTLY MEDIATED ACCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(05)_ODP	***systems or system components that implement the security design principle of efficiently mediated access are defined;***

SA-08(05)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | EFFICIENTLY MEDIATED ACCESS	
	SA-08(05)	***<SA-08(05)_ODP systems or system components>*** implement the security design principle of efficiently mediated access.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(05)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of efficiently mediated access used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(05)-Interview	[SELECT FROM: Organizational personnel with acquisition/contracting responsibilities; organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(05)-Test	[SELECT FROM: Organizational processes for applying the security design principle of efficiently mediated access in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of efficiently mediated access in system specification, design, development, implementation, and modification].

SA-08(06)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MINIMIZED SHARING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(06)_ODP	***systems or system components that implement the security design principle of minimized sharing are defined;***
	SA-08(06)	***<SA-08(06)_ODP systems or system components>*** implement the security design principle of minimized sharing.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(06)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of minimized sharing used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(06)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(06)-Test	[SELECT FROM: Organizational processes for applying the security design principle of minimized sharing in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of minimized sharing in system specification, design, development, implementation, and modification].

SA-08(07)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | REDUCED COMPLEXITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(07)_ODP	***systems or system components that implement the security design principle of reduced complexity are defined;***
	SA-08(07)	***<SA-08(07)_ODP systems or system components>*** implement the security design principle of reduced complexity.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(07)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of reduced complexity used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(07)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(07)-Test	[SELECT FROM: Organizational processes for applying the security design principle of reduced complexity in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of reduced complexity in system specification, design, development, implementation, and modification].

SA-08(08)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE EVOLVABILITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(08)_ODP	***systems or system components that implement the security design principle of secure evolvability are defined;***
	SA-08(08)	***<SA-08(08)_ODP systems or system components>*** implement the security design principle of secure evolvability.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(08)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of secure evolvability used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(08)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].

SA-08(08)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE EVOLVABILITY	
	SA-08(08)-Test	[SELECT FROM: Organizational processes for applying the security design principle of secure evolvability in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of secure evolvability in system specification, design, development, implementation, and modification].

SA-08(09)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | TRUSTED COMPONENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(09)_ODP	***systems or system components that implement the security design principle of trusted components are defined;***
	SA-08(09)	***<SA-08(09)_ODP systems or system components>*** implement the security design principle of trusted components.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(09)-Examine	[SELECT FROM: Supply chain risk management plan; system and services acquisition policy; procedures addressing the security design principle of trusted components used in the specification, design, development, implementation, and modification of the system; system design documentation; security, supply chain risk management, and privacy requirements and specifications for the system; system security and privacy architecture; procedures for determining component assurance; system security plan; other relevant documents or records].
	SA-08(09)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities].
	SA-08(09)-Test	[SELECT FROM: Organizational processes for applying the security design principle of trusted components in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of trusted components in system specification, design, development, implementation, and modification].

SA-08(10)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | HIERARCHICAL TRUST	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(10)_ODP	***systems or system components that implement the security design principle of hierarchical trust are defined;***
	SA-08(10)	***<SA-08(10)_ODP systems or system components>*** implement the security design principle of hierarchical trust.

SA-08(10)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | HIERARCHICAL TRUST	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(10)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of hierarchical trust used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(10)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(10)-Test	[SELECT FROM: Organizational processes for applying the security design principle of hierarchical trust in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of hierarchical trust in system specification, design, development, implementation, and modification].

SA-08(11)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | INVERSE MODIFICATION THRESHOLD	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(11)_ODP	***systems or system components that implement the security design principle of inverse modification threshold are defined;***
	SA-08(11)	***<SA-08(11)_ODP systems or system components>*** implement the security design principle of inverse modification threshold.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(11)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of inverse modification threshold used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(11)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(11)-Test	[SELECT FROM: Organizational processes for applying the security design principle of inverse modification threshold in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of inverse modification threshold in system specification, design, development, implementation, and modification].

SA-08(12)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | HIERARCHICAL PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(12)_ODP	***systems or system components that implement the security design principle of hierarchical protection are defined;***
	SA-08(12)	***<SA-08(12)_ODP systems or system components>*** implement the security design principle of hierarchical protection.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(12)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of hierarchical protection used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(12)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(12)-Test	[SELECT FROM: Organizational processes for applying the security design principle of hierarchical protection in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of hierarchical protection in system specification, design, development, implementation, and modification].

SA-08(13)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MINIMIZED SECURITY ELEMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(13)_ODP	***systems or system components that implement the security design principle of minimized security elements are defined;***
	SA-08(13)	***<SA-08(13)_ODP systems or system components>*** implement the security design principle of minimized security elements.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(13)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of minimized security elements used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(13)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].

SA-08(13)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MINIMIZED SECURITY ELEMENTS	
	SA-08(13)-Test	[SELECT FROM: Organizational processes for applying the security design principle of minimized security elements in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of minimized security elements in system specification, design, development, implementation, and modification].

SA-08(14)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | LEAST PRIVILEGE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(14)_ODP	***systems or system components that implement the security design principle of least privilege are defined;***
	SA-08(14)	***<SA-08(14)_ODP systems or system components>*** implement the security design principle of least privilege.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(14)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of least privilege used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(14)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(14)-Test	[SELECT FROM: Organizational processes for applying the security design principle of least privilege in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of least privilege in system specification, design, development, implementation, and modification].

SA-08(15)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | PREDICATE PERMISSION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(15)_ODP	***systems or system components that implement the security design principle of predicate permission are defined;***
	SA-08(15)	***<SA-08(15)_ODP systems or system components>*** implement the security design principle of predicate permission.

SA-08(15)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | PREDICATE PERMISSION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(15)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of predicate permission used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(15)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(15)-Test	[SELECT FROM: Organizational processes for applying the security design principle of predicate permission in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of predicate permission in system specification, design, development, implementation, and modification].

SA-08(16)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SELF-RELIANT TRUSTWORTHINESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(16)_ODP	***systems or system components that implement the security design principle of self-reliant trustworthiness are defined;***
	SA-08(16)	***<SA-08(16)_ODP systems or system components>*** implement the security design principle of self-reliant trustworthiness.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(16)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of self-reliant trustworthiness used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(16)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(16)-Test	[SELECT FROM: Organizational processes for applying the security design principle of self-reliant trustworthiness in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of self-reliant trustworthiness in system specification, design, development, implementation, and modification].

SA-08(17)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE DISTRIBUTED COMPOSITION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(17)_ODP	***systems or system components that implement the security design principle of secure distributed composition are defined;***
	SA-08(17)	***<SA-08(17)_ODP systems or system components>*** implement the security design principle of secure distributed composition.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(17)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of secure distributed composition used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(17)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(17)-Test	[SELECT FROM: Organizational processes for applying the security design principle of secure distributed composition in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of secure distributed composition in system specification, design, development, implementation, and modification].

SA-08(18)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | TRUSTED COMMUNICATIONS CHANNELS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(18)_ODP	***systems or system components that implement the security design principle of trusted communications channels are defined;***
	SA-08(18)	***<SA-08(18)_ODP systems or system components>*** implement the security design principle of trusted communications channels.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(18)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of trusted communications channels used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(18)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].

SA-08(18)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | TRUSTED COMMUNICATIONS CHANNELS	
	SA-08(18)-Test	[SELECT FROM: Organizational processes for applying the security design principle of trusted communications channels in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of trusted communications channels in system specification, design, development, implementation, and modification].

SA-08(19)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | CONTINUOUS PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(19)_ODP	***systems or system components that implement the security design principle of continuous protection are defined;***
	SA-08(19)	***<SA-08(19)_ODP systems or system components>*** implement the security design principle of continuous protection.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(19)-Examine	[SELECT FROM: System and services acquisition policy; access control policy; system and communications protection policy; procedures addressing boundary protection; procedures addressing the security design principle of continuous protection used in the specification, design, development, implementation, and modification of the system; system configuration settings and associated documentation; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(19)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; organizational personnel with access enforcement responsibilities; system/network administrators; system developers; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities].
	SA-08(19)-Test	[SELECT FROM: Organizational processes for applying the security design principle of continuous protection in system specification, design, development, implementation, and modification; mechanisms implementing access enforcement functions; mechanisms supporting the application of the security design principle of continuous protection in system specification, design, development, implementation, and modification; mechanisms supporting and/or implementing secure failure].

SA-08(20)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE METADATA MANAGEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(20)_ODP	***systems or system components that implement the security design principle of secure metadata management are defined;***

SA-08(20)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE METADATA MANAGEMENT	
	SA-08(20)	***<SA-08(20)_ODP systems or system components>*** implement the security design principle of secure metadata management.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(20)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of metadata management used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(20)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(20)-Test	[SELECT FROM: Organizational processes for applying the security design principle of metadata management in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of metadata management in system specification, design, development, implementation, and modification].

SA-08(21)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SELF-ANALYSIS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(21)_ODP	***systems or system components that implement the security design principle of self-analysis are defined;***
	SA-08(21)	***<SA-08(21)_ODP systems or system components>*** implement the security design principle of self-analysis.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(21)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of self-analysis used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(21)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(21)-Test	[SELECT FROM: Organizational processes for applying the security design principle of self-analysis in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of self-analysis in system specification, design, development, implementation, and modification].

SA-08(22)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | ACCOUNTABILITY AND TRACEABILITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(22)_ODP[01]	***systems or system components that implement the security design principle of accountability are defined;***
	SA-08(22)_ODP[02]	***systems or system components that implement the security design principle of traceability are defined;***
	SA-08(22)[01]	***<SA-08(22)_ODP[01] systems or system components>*** implement the security design principle of accountability;
	SA-08(22)[02]	***<SA-08(22)_ODP[02] systems or system components>*** implement the security design principle of traceability.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(22)-Examine	[SELECT FROM: System and services acquisition policy; audit and accountability policy; access control policy; procedures addressing least privilege; procedures addressing auditable events; identification and authentication policy; procedures addressing user identification and authentication; procedures addressing the security design principle of accountability and traceability used in the specification, design, development, implementation, and modification of the system; system design documentation; system audit records; system auditable events; system configuration settings and associated documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(22)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with audit and accountability responsibilities; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(22)-Test	[SELECT FROM: Organizational processes for applying the security design principle of accountability and traceability in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of accountability and traceability in system specification, design, development, implementation, and modification; mechanisms implementing information system auditing; mechanisms implementing least privilege functions].

SA-08(23)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE DEFAULTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(23)_ODP	***systems or system components that implement the security design principle of secure defaults are defined;***
	SA-08(23)	***<SA-08(23)_ODP systems or system components>*** implement the security design principle of secure defaults.

SA-08(23)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE DEFAULTS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(23)-Examine	[SELECT FROM: System and services acquisition policy; configuration management policy; procedures addressing the security design principle of secure defaults used in the specification, design, development, implementation, and modification of the system; system design documentation; procedures addressing the baseline configuration of the system; configuration management plan; system architecture and configuration documentation; system configuration settings and associated documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; procedures addressing system documentation; system documentation; system security plan; other relevant documents or records].
	SA-08(23)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(23)-Test	[SELECT FROM: Organizational processes for applying the security design principle of secure defaults in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of secure defaults in system specification, design, development, implementation, and modification; organizational processes for managing baseline configurations; mechanisms supporting configuration control of the baseline configuration].

SA-08(24)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE FAILURE AND RECOVERY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(24)_ODP[01]	***systems or system components that implement the security design principle of secure failure are defined;***
	SA-08(24)_ODP[02]	***systems or system components that implement the security design principle of secure recovery are defined;***
	SA-08(24)[01]	***<SA-08(24)_ODP[01] systems or system components>*** implement the security design principle of secure failure;
	SA-08(24)[02]	***<SA-08(24)_ODP[02] systems or system components>*** implement the security design principle of secure recovery.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(24)-Examine	[SELECT FROM: System and services acquisition policy; system and communications protection policy; contingency planning policy; procedures addressing information system recovery and reconstitution; procedures addressing the security design principle of secure failure and recovery used in the specification, design, development, implementation, and modification of the system; contingency plan; procedures addressing system backup; contingency plan test documentation; contingency plan test results; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].

SA-08(24)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE FAILURE AND RECOVERY	
	SA-08(24)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; organizational personnel with contingency plan testing responsibilities; organizational personnel with system recovery and reconstitution responsibilities; system developers; organizational personnel with information security responsibilities; organizational personnel with information system backup responsibilities].
	SA-08(24)-Test	[SELECT FROM: Organizational processes for applying the security design principle of secure failure and recovery in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of secure failure and recovery in system specification, design, development, implementation, and modification; mechanisms supporting and/or implementing secure failure; organizational processes for contingency plan testing; mechanisms supporting contingency plan testing; mechanisms supporting recovery and reconstitution of the system; organizational processes for conducting system backups; mechanisms supporting and/or implementing system backups].

SA-08(25)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | ECONOMIC SECURITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(25)_ODP	***systems or system components that implement the security design principle of economic security are defined;***
	SA-08(25)	***<SA-08(25)_ODP systems or system components>*** implement the security design principle of economic security.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(25)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of economic security used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; cost-benefit analysis; system security plan; other relevant documents or records].
	SA-08(25)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(25)-Test	[SELECT FROM: Organizational processes for applying the security design principle of economic security in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of economic security in system specification, design, development, implementation, and modification].

SA-08(26)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | PERFORMANCE SECURITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(26)_ODP	***systems or system components that implement the security design principle of performance security are defined;***
	SA-08(26)	***<SA-08(26)_ODP systems or system components>*** implement the security design principle of performance security.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(26)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of performance security used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; trade-off analysis between performance and security; system security plan; other relevant documents or records].
	SA-08(26)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(26)-Test	[SELECT FROM: Organizational processes for applying the security design principle of performance security in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of performance security in system specification, design, development, implementation, and modification].

SA-08(27)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | HUMAN FACTORED SECURITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(27)_ODP	***systems or system components that implement the security design principle of human factored security are defined;***
	SA-08(27)	***<SA-08(27)_ODP systems or system components>*** implement the security design principle of human factored security.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(27)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of human factored security used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; usability analysis; system security plan; other relevant documents or records].
	SA-08(27)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with human factored security responsibilities; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].

SA-08(27)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | HUMAN FACTORED SECURITY	
	SA-08(27)-Test	[SELECT FROM: Organizational processes for applying the security design principle of human factored security in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of human factored security in system specification, design, development, implementation, and modification; mechanisms that enforce security policies].

SA-08(28)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | ACCEPTABLE SECURITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(28)_ODP	***systems or system components that implement the security design principle of acceptable security are defined;***
	SA-08(28)	***<SA-08(28)_ODP systems or system components>*** implement the security design principle of acceptable security.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(28)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing the security design principle of acceptable security used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; personally identifiable information processing policy; privacy notifications provided to users; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SA-08(28)-Interview	[SELECT FROM: Organizational personnel with information security and privacy responsibilities; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers].
	SA-08(28)-Test	[SELECT FROM: Organizational processes for applying the security design principle of acceptable security in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of acceptable security in system specification, design, development, implementation, and modification; mechanisms that enforce security policies].

SA-08(29)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | REPEATABLE AND DOCUMENTED PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(29)_ODP	***systems or system components that implement the security design principle of repeatable and documented procedures are defined;***
	SA-08(29)	***<SA-08(29)_ODP systems or system components>*** implement the security design principle of repeatable and documented procedures.

SA-08(29)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | REPEATABLE AND DOCUMENTED PROCEDURES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(29)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of repeatable and documented procedures used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(29)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(29)-Test	[SELECT FROM: Organizational processes for applying the security design principle of repeatable and documented procedures in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of repeatable and documented procedures in system specification, design, development, implementation, and modification; mechanisms that enforce security policies].

SA-08(30)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | PROCEDURAL RIGOR	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(30)_ODP	***systems or system components that implement the security design principle of procedural rigor are defined;***
	SA-08(30)	***<SA-08(30)_ODP systems or system components>*** implement the security design principle of procedural rigor.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(30)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of procedural rigor used in the specification, design, development, implementation, and modification of the system; system design documentation; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(30)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(30)-Test	[SELECT FROM: Organizational processes for applying the security design principle of procedural rigor in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of procedural rigor in system specification, design, development, implementation, and modification; mechanisms that enforce security policies].

SA-08(31)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE SYSTEM MODIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(31)_ODP	***systems or system components that implement the security design principle of secure system modification are defined;***
	SA-08(31)	***<SA-08(31)_ODP systems or system components>*** implement the security design principle of secure system modification.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(31)-Examine	[SELECT FROM: System and services acquisition policy; configuration management policy and procedures; procedures addressing the security design principle of secure system modification used in the specification, design, development, implementation, and modification of the system; system design documentation; system configuration settings and associated documentation; change control records; security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; other relevant documents or records].
	SA-08(31)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(31)-Test	[SELECT FROM: Organizational processes for applying the security design principle of secure system modification in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of secure system modification in system specification, design, development, implementation, and modification; mechanisms that enforce security policies; organizational processes for managing change configuration; mechanisms supporting configuration control].

SA-08(32)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SUFFICIENT DOCUMENTATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(32)_ODP	***systems or system components that implement the security design principle of sufficient documentation are defined;***
	SA-08(32)	***<SA-08(32)_ODP systems or system components>*** implement the security design principle of sufficient documentation.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(32)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the security design principle of sufficient documentation used in the specification, design, development, implementation, and modification of the system; system design documentation; system configuration settings and associated documentation; change control records; security and privacy requirements and specifications for the system; system security and privacy documentation; system security and privacy architecture; system security plan; other relevant documents or records].

SA-08(32)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SUFFICIENT DOCUMENTATION	
	SA-08(32)-Interview	[SELECT FROM: Organizational personnel with the responsibility for determining system security and privacy requirements; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers; organizational personnel with information security responsibilities].
	SA-08(32)-Test	[SELECT FROM: Organizational processes for applying the security design principle of sufficient documentation in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of sufficient documentation in system specification, design, development, implementation, and modification; mechanisms that enforce security policies; organizational processes for managing change configuration; mechanisms supporting configuration control].

SA-08(33)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MINIMIZATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-08(33)_ODP	***processes that implement the privacy principle of minimization are defined;***
	SA-08(33)	the privacy principle of minimization is implemented using ***<SA-08(33)_ODP processes>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-08(33)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; personally identifiable information processing policy; procedures addressing the minimization of personally identifiable information in system design; system design documentation; system configuration settings and associated documentation; change control records; information security and privacy requirements and specifications for the system; system security and privacy architecture; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SA-08(33)-Interview	[SELECT FROM: Organizational personnel with information security and privacy responsibilities; organizational personnel with system specification, design, development, implementation, and modification responsibilities; system developers].
	SA-08(33)-Test	[SELECT FROM: Organizational processes for applying the privacy design principle of minimization in system specification, design, development, implementation, and modification; mechanisms supporting the application of the security design principle of sufficient documentation in system specification, design, development, implementation, and modification; mechanisms that enforce security and privacy policy; organizational processes for managing change configuration; mechanisms supporting configuration control].

SA-09	EXTERNAL SYSTEM SERVICES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-09_ODP[01]	***controls to be employed by external system service providers are defined;***
	SA-09_ODP[02]	***processes, methods, and techniques employed to monitor control compliance by external service providers are defined;***
	SA-09a.[01]	providers of external system services comply with organizational security requirements;
	SA-09a.[02]	providers of external system services comply with organizational privacy requirements;
	SA-09a.[03]	providers of external system services employ ***<SA-09_ODP[01] controls>***;
	SA-09b.[01]	organizational oversight with regard to external system services are defined and documented;
	SA-09b.[02]	user roles and responsibilities with regard to external system services are defined and documented;
	SA-09c.	***<SA-09_ODP[02] processes, methods, and techniques>*** are employed to monitor control compliance by external service providers on an ongoing basis.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-09-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing methods and techniques for monitoring control compliance by external service providers of system services; acquisition documentation; contracts; service level agreements; interagency agreements; licensing agreements; list of organizational security and privacy requirements for external provider services; control assessment results or reports from external providers of system services; system security plan; privacy plan; supply chain risk management plan; other relevant documents or records].
	SA-09-Interview	[SELECT FROM: Organizational personnel with acquisition responsibilities; external providers of system services; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities].
	SA-09-Test	[SELECT FROM: Organizational processes for monitoring security and privacy control compliance by external service providers on an ongoing basis; mechanisms for monitoring security and privacy control compliance by external service providers on an ongoing basis].

SA-09(01)	EXTERNAL SYSTEM SERVICES | RISK ASSESSMENTS AND ORGANIZATIONAL APPROVALS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-09(01)_ODP	***personnel or roles that approve the acquisition or outsourcing of dedicated information security services is/are defined;***
	SA-09(01)(a)	an organizational assessment of risk is conducted prior to the acquisition or outsourcing of information security services;

SA-09(01)	EXTERNAL SYSTEM SERVICES | RISK ASSESSMENTS AND ORGANIZATIONAL APPROVALS	
	SA-09(01)(b)	***<SA-09(01)_ODP personnel or roles>*** approve the acquisition or outsourcing of dedicated information security services.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-09(01)-Examine	[SELECT FROM: System and services acquisition policy; supply chain risk management policy and procedures; procedures addressing external system services; acquisition documentation; acquisition contracts for the system, system component, or system service; risk assessment reports; approval records for the acquisition or outsourcing of dedicated security services; system security plan; supply chain risk management plan; other relevant documents or records].
	SA-09(01)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with system security responsibilities; external providers of system services; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities].
	SA-09(01)-Test	[SELECT FROM: Organizational processes for conducting a risk assessment prior to acquiring or outsourcing dedicated security services; organizational processes for approving the outsourcing of dedicated security services; mechanisms supporting and/or implementing risk assessment; mechanisms supporting and/or implementing approval processes].

SA-09(02)	EXTERNAL SYSTEM SERVICES | IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-09(02)_ODP	***external system services that require the identification of functions, ports, protocols, and other services are defined;***
	SA-09(02)	providers of ***<SA-09(02)_ODP external system services>*** are required to identify the functions, ports, protocols, and other services required for the use of such services.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-09(02)-Examine	[SELECT FROM: System and services acquisition policy; supply chain risk management policy and procedures; procedures addressing external system services; acquisition contracts for the system, system component, or system service; acquisition documentation; solicitation documentation; service level agreements; organizational security requirements and security specifications for external service providers; list of required functions, ports, protocols, and other services; system security plan; other relevant documents or records].
	SA-09(02)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; system/network administrators; external providers of system services].

SA-09(03)	EXTERNAL SYSTEM SERVICES | ESTABLISH AND MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-09(03)_ODP[01]	***security requirements, properties, factors, or conditions defining acceptable trust relationships on which a trust relationship is maintained are defined;***
	SA-09(03)_ODP[02]	***privacy requirements, properties, factors, or conditions defining acceptable trust relationships on which a trust relationship is maintained are defined;***
	SA-09(03)[01]	trust relationships with external service provides based on ***<SA-09(03)_ODP[01] security requirements, properties, factors, or conditions>*** are established and documented;
	SA-09(03)[02]	trust relationships with external service provides based on ***<SA-09(03)_ODP[01] security requirements, properties, factors, or conditions>*** are maintained;
	SA-09(03)[03]	trust relationships with external service provides based on ***<SA-09(03)_ODP[02] privacy requirements, properties, factors, or conditions>*** are established and documented;
	SA-09(03)[04]	trust relationships with external service provides based on ***<SA-09(03)_ODP[02] privacy requirements, properties, factors, or conditions>*** are maintained.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-09(03)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; acquisition contracts for the system, system component, or system service; acquisition documentation; solicitation documentation; service level agreements; memorandum of understanding; memorandum of agreements; list of organizational security and privacy requirements, properties, factors, or conditions for external provider services; documentation of trust relationships with external service providers; system security plan; privacy plan; supply chain risk management plan; other relevant documents or records].
	SA-09(03)-Interview	[SELECT FROM: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities; external providers of system services; organizational personnel with supply chain risk management responsibilities].

SA-09(04)	EXTERNAL SYSTEM SERVICES | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-09(04)_ODP[01]	***external service providers are defined;***
	SA-09(04)_ODP[02]	***actions to be taken to verify that the interests of external service providers are consistent with and reflect organizational interests are defined;***
	SA-09(04)	***<SA-09(04)_ODP[02] actions>*** are taken to verify that the interests of ***<SA-09(04)_ODP[01] external service providers>*** are consistent with and reflect organizational interests.

SA-09(04)	EXTERNAL SYSTEM SERVICES | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-09(04)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing external system services; acquisition contracts for the system, system component, or system service; solicitation documentation; acquisition documentation; service level agreements; organizational security requirements/safeguards for external service providers; personnel security policies for external service providers; assessments performed on external service providers; system security plan; supply chain risk management plan; other relevant documents or records].
	SA-09(04)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; external providers of system services; organizational personnel with supply chain risk management responsibilities].
	SA-09(04)-Test	[SELECT FROM: Organizational processes for defining and employing safeguards to ensure consistent interests with external service providers; mechanisms supporting and/or implementing safeguards to ensure consistent interests with external service providers].

SA-09(05)	EXTERNAL SYSTEM SERVICES | PROCESSING, STORAGE, AND SERVICE LOCATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-09(05)_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {information processing; information or data; system services};***
	SA-09(05)_ODP[02]	***locations where <SA-09(05)_ODP[01] SELECTED PARAMETER VALUE(S)> is/are to be restricted are defined;***
	SA-09(05)_ODP[03]	***requirements or conditions for restricting the location of <SA-09(05)_ODP[01] SELECTED PARAMETER VALUE(S)> are defined;***
	SA-09(05)	based on ***<SA-09(05)_ODP[03] requirements>***, ***<SA-09(05)_ODP[01] SELECTED PARAMETER VALUE(S)>*** is/are restricted to ***<SA-09(05)_ODP[02] locations>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-09(05)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing external system services; acquisition contracts for the system, system component, or system service; solicitation documentation; acquisition documentation; service level agreements; restricted locations for information processing; information/data and/or system services; information processing, information/data, and/or system services to be maintained in restricted locations; organizational security requirements or conditions for external providers; system security plan; supply chain risk management plan; other relevant documents or records].
	SA-09(05)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; external providers of system services; organizational personnel with supply chain risk management responsibilities].

SA-09(05)	EXTERNAL SYSTEM SERVICES | PROCESSING, STORAGE, AND SERVICE LOCATION	
	SA-09(05)-Test	[SELECT FROM: Organizational processes for defining the requirements to restrict locations of information processing, information/data, or information services; organizational processes for ensuring the location is restricted in accordance with requirements or conditions].

SA-09(06)	EXTERNAL SYSTEM SERVICES | ORGANIZATION-CONTROLLED CRYPTOGRAPHIC KEYS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-09(06)	exclusive control of cryptographic keys is maintained for encrypted material stored or transmitted through an external system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-09(06)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing external system services; acquisition contracts for the system, system component, or system service; solicitation documentation; acquisition documentation; service level agreements; procedures addressing organization-controlled cryptographic key management; organizational security requirements or conditions for external providers; system security plan; supply chain risk management plan; other relevant documents or records].
	SA-09(06)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organization personnel with cryptographic key management responsibilities; external providers of system services; organizational personnel with supply chain risk management responsibilities].
	SA-09(06)-Test	[SELECT FROM: Organizational processes for cryptographic key management; mechanisms for supporting and implementing the management of organization-controlled cryptographic keys].

SA-09(07)	EXTERNAL SYSTEM SERVICES | ORGANIZATION-CONTROLLED INTEGRITY CHECKING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-09(07)	the capability is provided to check the integrity of information while it resides in the external system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-09(07)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing external system services; acquisition contracts for the system, system component, or system service; solicitation documentation; acquisition documentation; service level agreements; procedures addressing organization-controlled integrity checking; information/data and/or system services; organizational security requirements or conditions for external providers; system security plan; supply chain risk management plan; other relevant documents or records].

SA-09(07)	EXTERNAL SYSTEM SERVICES | ORGANIZATION-CONTROLLED INTEGRITY CHECKING	
	SA-09(07)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organization personnel with integrity checking responsibilities; external providers of system services; organizational personnel with supply chain risk management responsibilities].
	SA-09(07)-Test	[SELECT FROM: Organizational processes for integrity checking; mechanisms for supporting and implementing integrity checking of information in external systems].

SA-09(08)	EXTERNAL SYSTEM SERVICES | PROCESSING AND STORAGE LOCATION — U.S. JURISDICTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-09(08)	the geographic location of information processing and data storage is restricted to facilities located within the legal jurisdictional boundary of the United States.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-09(08)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing external system services; acquisition contracts for the system, system component, or system service; solicitation documentation; acquisition documentation; service level agreements; procedures addressing determining jurisdiction restrictions for processing and storage location; information/data and/or system services; organizational security requirements or conditions for external providers; system security plan; supply chain risk management plan; other relevant documents or records].
	SA-09(08)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organization personnel with supply chain risk management responsibilities; external providers of system services].
	SA-09(08)-Test	[SELECT FROM: Organizational processes restricting external system service providers to process and store information within the legal jurisdictional boundary of the United States].

SA-10	DEVELOPER CONFIGURATION MANAGEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-10_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {design; development; implementation; operation; disposal};***
	SA-10_ODP[02]	***configuration items under configuration management are defined;***
	SA-10_ODP[03]	***personnel to whom security flaws and flaw resolutions within the system, component, or service are reported is/are defined;***

SA-10	DEVELOPER CONFIGURATION MANAGEMENT	
	SA-10a.	the developer of the system, system component, or system service is required to perform configuration management during system, component, or service ***<SA-10_ODP[01] SELECTED PARAMETER VALUE(S)>***;
	SA-10b.[01]	the developer of the system, system component, or system service is required to document the integrity of changes to ***<SA-10_ODP[02] configuration items>***;
	SA-10b.[02]	the developer of the system, system component, or system service is required to manage the integrity of changes to ***<SA-10_ODP[02] configuration items>***;
	SA-10b.[03]	the developer of the system, system component, or system service is required to control the integrity of changes to ***<SA-10_ODP[02] configuration items>***;
	SA-10c.	the developer of the system, system component, or system service is required to implement only organization-approved changes to the system, component, or service;
	SA-10d.[01]	the developer of the system, system component, or system service is required to document approved changes to the system, component, or service;
	SA-10d.[02]	the developer of the system, system component, or system service is required to document the potential security impacts of approved changes;
	SA-10d.[03]	the developer of the system, system component, or system service is required to document the potential privacy impacts of approved changes;
	SA-10e.[01]	the developer of the system, system component, or system service is required to track security flaws within the system, component, or service;
	SA-10e.[02]	the developer of the system, system component, or system service is required to track security flaw resolutions within the system, component, or service;
	SA-10e.[03]	the developer of the system, system component, or system service is required to report findings to ***<SA-10_ODP[03] personnel>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-10-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing system developer configuration management; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer configuration management plan; security flaw and flaw resolution tracking records; system change authorization records; change control records; configuration management records; system security plan; other relevant documents or records].
	SA-10-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with configuration management responsibilities; system developers].
	SA-10-Test	[SELECT FROM: Organizational processes for monitoring developer configuration management; mechanisms supporting and/or implementing the monitoring of developer configuration management].

SA-10(01)	DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE AND FIRMWARE INTEGRITY VERIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-10(01)	the developer of the system, system component, or system service is required to enable integrity verification of software and firmware components.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-10(01)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing system developer configuration management; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer configuration management plan; software and firmware integrity verification records; system change authorization records; change control records; configuration management records; system security plan; supply chain risk management plan; other relevant documents or records].
	SA-10(01)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with configuration management responsibilities; system developers; organizational personnel with supply chain risk management responsibilities].
	SA-10(01)-Test	[SELECT FROM: Organizational processes for monitoring developer configuration management; mechanisms supporting and/or implementing the monitoring of developer configuration management].

SA-10(02)	DEVELOPER CONFIGURATION MANAGEMENT | ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-10(02)	an alternate configuration management process has been provided using organizational personnel in the absence of a dedicated developer configuration management team.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-10(02)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; configuration management policy; configuration management plan; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer configuration management plan; security impact analyses; privacy impact analyses; privacy impact assessment; privacy risk assessment documentation; system security plan; privacy plan; other relevant documents or records].
	SA-10(02)-Interview	[SELECT FROM: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with configuration management responsibilities; system developers].

SA-10(02)	DEVELOPER CONFIGURATION MANAGEMENT | ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES	
	SA-10(02)-Test	[SELECT FROM: Organizational processes for monitoring developer configuration management; mechanisms supporting and/or implementing the monitoring of developer configuration management].

SA-10(03)	DEVELOPER CONFIGURATION MANAGEMENT | HARDWARE INTEGRITY VERIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-10(03)	the developer of the system, system component, or system service is required to enable integrity verification of hardware components.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-10(03)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing system developer configuration management; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer configuration management plan; hardware integrity verification records; system security plan; supply chain risk management plan; other relevant documents or records].
	SA-10(03)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with configuration management responsibilities; system developers; organizational personnel with supply chain risk management responsibilities].
	SA-10(03)-Test	[SELECT FROM: Organizational processes for monitoring developer configuration management; mechanisms supporting and/or implementing the monitoring of developer configuration management].

SA-10(04)	DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED GENERATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-10(04)[01]	the developer of the system, system component, or system service is required to employ tools for comparing newly generated versions of security-relevant hardware descriptions with previous versions;
	SA-10(04)[02]	the developer of the system, system component, or system service is required to employ tools for comparing newly generated versions of source code with previous versions;
	SA-10(04)[03]	the developer of the system, system component, or system service is required to employ tools for comparing newly generated versions of object code with previous versions.

SA-10(04)	DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED GENERATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-10(04)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing system developer configuration management; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer configuration management plan; change control records; configuration management records; configuration control audit records; system security plan; other relevant documents or records].
	SA-10(04)-Test	[SELECT FROM: Organizational processes for monitoring developer configuration management; mechanisms supporting and/or implementing the monitoring of developer configuration management].

SA-10(05)	DEVELOPER CONFIGURATION MANAGEMENT | MAPPING INTEGRITY FOR VERSION CONTROL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-10(05)	the developer of the system, system component, or system service is required to maintain the integrity of the mapping between the master build data describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-10(05)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing system developer configuration management; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer configuration management plan; change control records; configuration management records; version control change/update records; integrity verification records between master copies of security-relevant hardware, software, and firmware (including designs and source code); system security plan; other relevant documents or records].
	SA-10(05)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with configuration management responsibilities; system developers].
	SA-10(05)-Test	[SELECT FROM: Organizational processes for monitoring developer configuration management; mechanisms supporting and/or implementing the monitoring of developer configuration management].

SA-10(06)	DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED DISTRIBUTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-10(06)	the developer of the system, system component, or system service is required to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-10(06)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing system developer configuration management; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer configuration management plan; change control records; configuration management records; system security plan; other relevant documents or records].
	SA-10(06)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with configuration management responsibilities; system developers].
	SA-10(06)-Test	[SELECT FROM: Organizational processes for monitoring developer configuration management; mechanisms supporting and/or implementing the monitoring of developer configuration management].

SA-10(07)	DEVELOPER CONFIGURATION MANAGEMENT | SECURITY AND PRIVACY REPRESENTATIVES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-10(07)_ODP[01]	***security representatives to be included in the configuration change management and control process are defined;***
	SA-10(07)_ODP[02]	***privacy representatives to be included in the configuration change management and control process are defined;***
	SA-10(07)_ODP[03]	***configuration change management and control processes in which security representatives are required to be included are defined;***
	SA-10(07)_ODP[04]	***configuration change management and control processes in which privacy representatives are required to be included are defined;***
	SA-10(07)[01]	***<SA-10(07)_ODP[01] security representatives>*** are required to be included in the ***<SA-10(07)_ODP[03] configuration change management and control processes>***;
	SA-10(07)[02]	***<SA-10(07)_ODP[02] privacy representatives>*** are required to be included in the ***<SA-10(07)_ODP[04] configuration change management and control processes>***.

SA-10(07)	DEVELOPER CONFIGURATION MANAGEMENT | SECURITY AND PRIVACY REPRESENTATIVES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-10(07)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; configuration management policy; configuration management plan; solicitation documentation requiring representatives for security and privacy; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer configuration management plan; change control records; configuration management records; system security plan; other relevant documents or records].
	SA-10(07)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with configuration management responsibilities; system developers].

SA-11	DEVELOPER TESTING AND EVALUATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-11_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {unit; integration; system; regression};***
	SA-11_ODP[02]	***frequency at which to conduct <SA-11_ODP[01] SELECTED PARAMETER VALUE(S)> testing/evaluation is defined;***
	SA-11_ODP[03]	***depth and coverage of <SA-11_ODP[01] SELECTED PARAMETER VALUE(S)> testing/evaluation is defined;***
	SA-11a.[01]	the developer of the system, system component, or system service is required at all post-design stages of the system development life cycle to develop a plan for ongoing security assessments;
	SA-11a.[02]	the developer of the system, system component, or system service is required at all post-design stages of the system development life cycle to implement a plan for ongoing security assessments;
	SA-11a.[03]	the developer of the system, system component, or system service is required at all post-design stages of the system development life cycle to develop a plan for privacy assessments;
	SA-11a.[04]	the developer of the system, system component, or system service is required at all post-design stages of the system development life cycle to implement a plan for ongoing privacy assessments;
	SA-11b.	the developer of the system, system component, or system service is required at all post-design stages of the system development life cycle to perform ***<SA-11_ODP[01] SELECTED PARAMETER VALUE(S)>*** testing/evaluation ***<SA-11_ODP[02] frequency to conduct>*** at ***<SA-11_ODP[03] depth and coverage>***;
	SA-11c.[01]	the developer of the system, system component, or system service is required at all post-design stages of the system development life cycle to produce evidence of the execution of the assessment plan;

SA-11	DEVELOPER TESTING AND EVALUATION	
	SA-11c.[02]	the developer of the system, system component, or system service is required at all post-design stages of the system development life cycle to produce the results of the testing and evaluation;
	SA-11d.	the developer of the system, system component, or system service is required at all post-design stages of the system development life cycle to implement a verifiable flaw remediation process;
	SA-11e.	the developer of the system, system component, or system service is required at all post-design stages of the system development life cycle to correct flaws identified during testing and evaluation.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-11-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing system developer security and privacy testing; procedures addressing flaw remediation; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; security and privacy architecture; system design documentation; system developer security and privacy assessment plans; results of developer security and privacy assessments for the system, system component, or system service; security and privacy flaw and remediation tracking records; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SA-11-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with developer security and privacy testing responsibilities; system developers].
	SA-11-Test	[SELECT FROM: Organizational processes for monitoring developer security testing and evaluation; mechanisms supporting and/or implementing the monitoring of developer security and privacy testing and evaluation].

SA-11(01)	DEVELOPER TESTING AND EVALUATION | STATIC CODE ANALYSIS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-11(01)[01]	the developer of the system, system component, or system service is required to employ static code analysis tools to identify common flaws;
	SA-11(01)[02]	the developer of the system, system component, or system service is required to employ static code analysis tools to document the results of the analysis.

SA-11(01)	DEVELOPER TESTING AND EVALUATION | STATIC CODE ANALYSIS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-11(01)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing system developer security testing; procedures addressing flaw remediation; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; security and privacy architecture; system design documentation; system developer security and privacy assessment plans; results of system developer security and privacy assessments; security flaw and remediation tracking records; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SA-11(01)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with developer security and privacy testing responsibilities; organizational personnel with configuration management responsibilities; system developers].
	SA-11(01)-Test	[SELECT FROM: Organizational processes for monitoring developer security testing and evaluation; mechanisms supporting and/or implementing the monitoring of developer security testing and evaluation; static code analysis tools].

SA-11(02)	DEVELOPER TESTING AND EVALUATION | THREAT MODELING AND VULNERABILITY ANALYSES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-11(02)_ODP[01]	***information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels to be used as contextual information for threat modeling and vulnerability analyses is defined;***
	SA-11(02)_ODP[02]	***the tools and methods to be employed for threat modeling and vulnerability analyses are defined;***
	SA-11(02)_ODP[03]	***the breadth and depth of threat modeling to be conducted is defined;***
	SA-11(02)_ODP[04]	***the breadth and depth of vulnerability analyses to be conducted is defined;***
	SA-11(02)_ODP[05]	***acceptance criteria to be met by produced evidence for threat modeling are defined;***
	SA-11(02)_ODP[06]	***acceptance criteria to be met by produced evidence for vulnerability analyses are defined;***
	SA-11(02)(a)[01]	the developer of the system, system component, or system service is required to perform threat modeling during development of the system, component, or service that uses ***<SA-11(02)_ODP[01] information>***;
	SA-11(02)(a)[02]	the developer of the system, system component, or system service is required to perform vulnerability analyses during development of the system, component, or service that uses ***<SA-11(02)_ODP[01] information>***;
	SA-11(02)(a)[03]	the developer of the system, system component, or system service is required to perform threat modeling during the subsequent testing and evaluation of the system, component, or service that uses ***<SA-11(02)_ODP[01] information>***;

SA-11(02)	DEVELOPER TESTING AND EVALUATION | THREAT MODELING AND VULNERABILITY ANALYSES	
	SA-11(02)(a)[04]	the developer of the system, system component, or system service is required to perform vulnerability analyses during the subsequent testing and evaluation of the system, component, or service that uses ***<SA-11(02)_ODP[01] information>***;
	SA-11(02)(b)[01]	the developer of the system, system component, or system service is required to perform threat modeling during development of the system, component, or service that employs ***<SA-11(02)_ODP[02] tools and methods>***;
	SA-11(02)(b)[02]	the developer of the system, system component, or system service is required to perform threat modeling during the subsequent testing and evaluation of the system, component, or service that employs ***<SA-11(02)_ODP[02] tools and methods>***;
	SA-11(02)(b)[03]	the developer of the system, system component, or system service is required to perform vulnerability analyses during development of the system, component, or service that employs ***<SA-11(02)_ODP[02] tools and methods>***;
	SA-11(02)(b)[04]	the developer of the system, system component, or system service is required to perform vulnerability analyses during the subsequent testing and evaluation of the system, component, or service that employs ***<SA-11(02)_ODP[02] tools and methods>***;
	SA-11(02)(c)[01]	the developer of the system, system component, or system service is required to perform threat modeling at ***<SA-11(02)_ODP[03] breadth and depth>*** during development of the system, component, or service;
	SA-11(02)(c)[02]	the developer of the system, system component, or system service is required to perform vulnerability analyses during the subsequent testing and evaluation of the system, component, or service that conducts modeling and analyses at ***<SA-11(02)_ODP[04] breadth and depth>***;
	SA-11(02)(d)[01]	the developer of the system, system component, or system service is required to perform threat modeling during development of the system, component, or service that produces evidence that meets ***<SA-11(02)_ODP[05] acceptance criteria>***;
	SA-11(02)(d)[02]	the developer of the system, system component, or system service is required to perform threat modeling during the subsequent testing and evaluation of the system, component, or service that produces evidence that meets ***<SA-11(02)_ODP[05] acceptance criteria>***;
	SA-11(02)(d)[03]	the developer of the system, system component, or system service is required to perform vulnerability analyses during development of the system, component, or service that produces evidence that meets ***<SA-11(02)_ODP[06] acceptance criteria>***;
	SA-11(02)(d)[04]	the developer of the system, system component, or system service is required to perform vulnerability analyses during the subsequent testing and evaluation of the system, component, or service that produces evidence that meets ***<SA-11(02)_ODP[06] acceptance criteria>***.

SA-11(02)	DEVELOPER TESTING AND EVALUATION | THREAT MODELING AND VULNERABILITY ANALYSES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-11(02)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing system developer security testing; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer security test plans; records of developer security testing results for the system, system component, or system service; vulnerability scanning results; system risk assessment reports; threat and vulnerability analysis reports; system security plan; supply chain risk management plan; other relevant documents or records].
	SA-11(02)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with developer security testing responsibilities; system developers; organizational personnel with supply chain risk management responsibilities].
	SA-11(02)-Test	[SELECT FROM: Organizational processes for monitoring developer security testing and evaluation; mechanisms supporting and/or implementing the monitoring of developer security testing and evaluation].

SA-11(03)	DEVELOPER TESTING AND EVALUATION | INDEPENDENT VERIFICATION OF ASSESSMENT PLANS AND EVIDENCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-11(03)_ODP	***independence criteria to be satisfied by an independent agent are defined;***
	SA-11(03)(a)[01]	an independent agent is required to satisfy ***<SA-11(03)_ODP independence criteria>*** to verify the correct implementation of the developer security assessment plan and the evidence produced during testing and evaluation;
	SA-11(03)(a)[02]	an independent agent is required to satisfy ***<SA-11(03)_ODP independence criteria>*** to verify the correct implementation of the developer privacy assessment plan and the evidence produced during testing and evaluation;
	SA-11(03)(b)	the independent agent is provided with sufficient information to complete the verification process or granted the authority to obtain such information.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-11(03)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing system developer security testing; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; independent verification and validation reports; security and privacy assessment plans; results of security and privacy assessments for the system, system component, or system service; system security plan; privacy plan; privacy program plan; other relevant documents or records].
	SA-11(03)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with developer security testing responsibilities; system developers; independent verification agent].

SA-11(03)	DEVELOPER TESTING AND EVALUATION | INDEPENDENT VERIFICATION OF ASSESSMENT PLANS AND EVIDENCE	
	SA-11(03)-Test	[SELECT FROM: Organizational processes for monitoring developer security testing and evaluation; mechanisms supporting and/or implementing the monitoring of developer security testing and evaluation].

SA-11(04)	DEVELOPER TESTING AND EVALUATION | MANUAL CODE REVIEWS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-11(04)_ODP[01]	***specific code requiring manual code review is defined;***
	SA-11(04)_ODP[02]	***processes, procedures, and/or techniques used for manual code reviews are defined;***
	SA-11(04)	the developer of the system, system component, or system service is required to perform a manual code review of ***<SA-11(04)_ODP[01] specific code>*** using ***<SA-11(04)_ODP[02] processes, procedures, and/or techniques>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-11(04)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing system developer security testing; processes, procedures, and/or techniques for performing manual code reviews; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer security testing and evaluation plans; system developer security testing and evaluation results; list of code requiring manual reviews; records of manual code reviews; system security plan; other relevant documents or records].
	SA-11(04)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with developer security testing responsibilities; system developers; independent verification agent].
	SA-11(04)-Test	[SELECT FROM: Organizational processes for monitoring developer security testing and evaluation; mechanisms supporting and/or implementing the monitoring of developer testing and evaluation].

SA-11(05)	DEVELOPER TESTING AND EVALUATION | PENETRATION TESTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-11(05)_ODP[01]	***the breadth of penetration testing is defined;***
	SA-11(05)_ODP[02]	***the depth of penetration testing is defined;***
	SA-11(05)_ODP[03]	***constraints of penetration testing are defined;***
	SA-11(05)(a)[01]	the developer of the system, system component, or system service is required to perform penetration testing at the following level of rigor: ***<SA-11(05)_ODP[01] breadth>***;

SA-11(05)	DEVELOPER TESTING AND EVALUATION | PENETRATION TESTING	
	SA-11(05)(a)[02]	the developer of the system, system component, or system service is required to perform penetration testing at the following level of rigor: ***<SA-11(05)_ODP[02] depth>***;
	SA-11(05)(b)	the developer of the system, system component, or system service is required to perform penetration testing under ***<SA-11(05)_ODP[03] constraints>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-11(05)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing system developer security testing; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer penetration testing and evaluation plans; system developer penetration testing and evaluation results; system security plan; privacy plan; personally identifiable information processing policy; other relevant documents or records].
	SA-11(05)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with developer security testing responsibilities; system developers; independent verification agent].
	SA-11(05)-Test	[SELECT FROM: Organizational processes for monitoring developer security and privacy assessments; mechanisms supporting and/or implementing the monitoring of developer security and privacy assessments].

SA-11(06)	DEVELOPER TESTING AND EVALUATION | ATTACK SURFACE REVIEWS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-11(06)	the developer of the system, system component, or system service is required to perform attack surface reviews.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-11(06)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing system developer security testing; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer security testing and evaluation plans; system developer security testing and evaluation results; records of attack surface reviews; system security plan; other relevant documents or records].
	SA-11(06)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with developer security testing responsibilities; organizational personnel with configuration management responsibilities; system developers].
	SA-11(06)-Test	[SELECT FROM: Organizational processes for monitoring developer security testing and evaluation; mechanisms supporting and/or implementing the monitoring of developer security testing and evaluation].

SA-11(07)	DEVELOPER TESTING AND EVALUATION | VERIFY SCOPE OF TESTING AND EVALUATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-11(07)_ODP[01]	***the breadth of testing and evaluation of required controls is defined;***
	SA-11(07)_ODP[02]	***the depth of testing and evaluation of required controls is defined;***
	SA-11(07)[01]	the developer of the system, system component, or system service is required to verify that the scope of testing and evaluation provides complete coverage of the required controls at ***<SA-11(07)_ODP[01] breadth>***;
	SA-11(07)[02]	the developer of the system, system component, or system service is required to verify that the scope of testing and evaluation provides complete coverage of the required controls at ***<SA-11(07)_ODP[02] depth>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-11(07)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing system developer security testing; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer security testing and evaluation plans; system developer security testing and evaluation results; system security plan; other relevant documents or records].
	SA-11(07)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with developer security testing responsibilities; system developers; independent verification agent].
	SA-11(07)-Test	[SELECT FROM: Organizational processes for monitoring developer security testing and evaluation; mechanisms supporting and/or implementing the monitoring of developer security testing and evaluation].

SA-11(08)	DEVELOPER TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-11(08)[01]	the developer of the system, system component, or system service is required to employ dynamic code analysis tools to identify common flaws;
	SA-11(08)[02]	the developer of the system, system component, or system service is required to document the results of the analysis.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-11(08)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing system developer security testing; procedures addressing flaw remediation; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer security test and evaluation plans; security test and evaluation results; security flaw and remediation tracking reports; system security plan; other relevant documents or records].

SA-11(08)	DEVELOPER TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS	
	SA-11(08)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with developer security testing responsibilities; organizational personnel with configuration management responsibilities; system developers].
	SA-11(08)-Test	[SELECT FROM: Organizational processes for monitoring developer security testing and evaluation; mechanisms supporting and/or implementing the monitoring of developer security testing and evaluation].

SA-11(09)	DEVELOPER TESTING AND EVALUATION | INTERACTIVE APPLICATION SECURITY TESTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-11(09)[01]	the developer of the system, system component, or system service is required to employ interactive application security testing tools to identify flaws;
	SA-11(09)[02]	the developer of the system, system component, or system service is required to document the results of flaw identification.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-11(09)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing system developer security testing; procedures addressing interactive application security testing; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer security test and evaluation plans; security test and evaluation results; security flaw and remediation tracking reports; system security plan; other relevant documents or records].
	SA-11(09)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with developer security testing responsibilities; organizational personnel with configuration management responsibilities; system developers].
	SA-11(09)-Test	[SELECT FROM: Organizational processes for interactive application security testing; mechanisms supporting and/or implementing interactive application security testing].

SA-12	SUPPLY CHAIN PROTECTION
	[WITHDRAWN: Incorporated into SR Family.]

SA-12(01)	SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS
	[WITHDRAWN: Moved to SR-05.]

SA-12(02)	SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS
	[WITHDRAWN: Moved to SR-06.]

SA-12(03)	SUPPLY CHAIN PROTECTION | TRUSTED SHIPPING AND WAREHOUSING
	[WITHDRAWN: Incorporated into SR-03.]

SA-12(04)	SUPPLY CHAIN PROTECTION | DIVERSITY OF SUPPLIERS
	[WITHDRAWN: Moved to SR-03(01).]

SA-12(05)	SUPPLY CHAIN PROTECTION | LIMITATION OF HARM
	[WITHDRAWN: Moved to SR-03(02).]

SA-12(06)	SUPPLY CHAIN PROTECTION | MINIMIZING PROCUREMENT TIME
	[WITHDRAWN: Incorporated into SR-05(01).]

SA-12(07)	SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE
	[WITHDRAWN: Moved to SR-05(02).]

SA-12(08)	SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE
	[WITHDRAWN: Incorporated into RA-03(02).]

SA-12(09)	SUPPLY CHAIN PROTECTION | OPERATIONS SECURITY
	[WITHDRAWN: Moved to SR-07.]

SA-12(10)	SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED
	[WITHDRAWN: Moved to SR-04(03).]

SA-12(11)	SUPPLY CHAIN PROTECTION | PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS
	[WITHDRAWN: Moved to SR-06(01).]

SA-12(12)	SUPPLY CHAIN PROTECTION | INTER-ORGANIZATIONAL AGREEMENTS
	[WITHDRAWN: Moved to SR-08.]

SA-12(13)	SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS
	[WITHDRAWN: Incorporated into MA-06, RA-09.]

SA-12(14)	SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY
	[WITHDRAWN: Incorporated into SR-04(01), SR-04(02).]

SA-12(15)	SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES
	[WITHDRAWN: Incorporated into SR-03.]

SA-13	TRUSTWORTHINESS
	[WITHDRAWN: Incorporated into SA-08.]

SA-14	CRITICALITY ANALYSIS
	[WITHDRAWN: Incorporated into RA-09.]

SA-14(01)	CRITICALITY ANALYSIS | CRITICAL COMPONENTS WITH NO VIABLE ALTERNATIVE SOURCING
	[WITHDRAWN: Incorporated into SA-20.]

SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-15_ODP[01]	***frequency at which to review the development process, standards, tools, tool options, and tool configurations is defined;***
	SA-15_ODP[02]	***security requirements to be satisfied by the process, standards, tools, tool options, and tool configurations are defined;***
	SA-15_ODP[03]	***privacy requirements to be satisfied by the process, standards, tools, tool options, and tool configurations are defined;***
	SA-15a.01[01]	the developer of the system, system component, or system service is required to follow a documented development process that explicitly addresses security requirements;
	SA-15a.01[02]	the developer of the system, system component, or system service is required to follow a documented development process that explicitly addresses privacy requirements;
	SA-15a.02[01]	the developer of the system, system component, or system service is required to follow a documented development process that identifies the standards used in the development process;
	SA-15a.02[02]	the developer of the system, system component, or system service is required to follow a documented development process that identifies the tools used in the development process;
	SA-15a.03[01]	the developer of the system, system component, or system service is required to follow a documented development process that documents the specific tool used in the development process;
	SA-15a.03[02]	the developer of the system, system component, or system service is required to follow a documented development process that documents the specific tool configurations used in the development process;
	SA-15a.04	the developer of the system, system component, or system service is required to follow a documented development process that documents, manages, and ensures the integrity of changes to the process and/or tools used in development;
	SA-15b.[01]	the developer of the system, system component, or system service is required to follow a documented development process in which the development process, standards, tools, tool options, and tool configurations are reviewed ***<SA-15_ODP[01] frequency>*** to determine that the process, standards, tools, tool options, and tool configurations selected and employed satisfy ***<SA-15_ODP[02] security requirements>***;
	SA-15b.[02]	the developer of the system, system component, or system service is required to follow a documented development process in which the development process, standards, tools, tool options, and tool configurations are reviewed ***<SA-15_ODP[01] frequency>*** to determine that the process, standards, tools, tool options, and tool configurations selected and employed satisfy ***<SA-15_ODP[03] privacy requirements>***.

SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-15-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing development process, standards, and tools; procedures addressing the integration of security and privacy requirements during the development process; solicitation documentation; acquisition documentation; critical component inventory documentation; service level agreements; acquisition contracts for the system, system component, or system service; system developer documentation listing tool options/configuration guides; configuration management policy; configuration management records; documentation of development process reviews using maturity models; change control records; configuration control records; documented reviews of the development process, standards, tools, and tool options/configurations; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SA-15-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security and privacy responsibilities; system developer].

SA-15(01)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | QUALITY METRICS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-15(01)_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {<SA-15(01)_ODP[02] frequency>; <SA-15(01)_ODP[03] program review>; upon delivery};***
	SA-15(01)_ODP[02]	***frequency at which to provide evidence of meeting the quality metrics is defined (if selected);***
	SA-15(01)_ODP[03]	***program review milestones are defined (if selected);***
	SA-15(01)(a)	the developer of the system, system component, or system service is required to define quality metrics at the beginning of the development process;
	SA-15(01)(b)	the developer of the system, system component, or system service is required to provide evidence of meeting the quality metrics ***<SA-15(01)_ODP[01] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-15(01)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing development process, standards, and tools; procedures addressing the integration of security requirements into the acquisition process; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; list of quality metrics; documentation evidence of meeting quality metrics; system security plan; other relevant documents or records].
	SA-15(01)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; system developer].

SA-15(02)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | SECURITY AND PRIVACY TRACKING TOOLS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-15(02)[01]	the developer of the system, system component, or system service is required to select and employ security tracking tools for use during the development process;
	SA-15(02)[02]	the developer of the system, system component, or system service is required to select and employ privacy tracking tools for use during the development process.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-15(02)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing development process, standards, and tools; procedures addressing the integration of security and privacy requirements into the acquisition process; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; documentation of the selection of security and privacy tracking tools; evidence of employing security and privacy tracking tools; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SA-15(02)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; system developer; organizational personnel with privacy responsibilities].

SA-15(03)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CRITICALITY ANALYSIS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-15(03)_ODP[01]	***decision points in the system development life cycle are defined;***
	SA-15(03)_ODP[02]	***the breadth of criticality analysis is defined;***
	SA-15(03)_ODP[03]	***the depth of criticality analysis is defined;***
	SA-15(03)(a)	the developer of the system, system component, or system service is required to perform a criticality analysis at ***<SA-15(03)_ODP[01] decision points>*** in the system development life cycle;
	SA-15(03)(b)[01]	the developer of the system, system component, or system service is required to perform a criticality analysis at the following rigor level: ***<SA-15(03)_ODP[02] breadth>***;
	SA-15(03)(b)[02]	the developer of the system, system component, or system service is required to perform a criticality analysis at the following rigor level: ***<SA-15(03)_ODP[03] depth>*** .

SA-15(03)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CRITICALITY ANALYSIS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-15(03)-Examine	[SELECT FROM: Supply chain risk management plan; system and services acquisition policy; procedures addressing development process, standards, and tools; procedures addressing criticality analysis requirements for the system, system component, or system service; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; criticality analysis documentation; business impact analysis documentation; software development life cycle documentation; system security plan; other relevant documents or records].
	SA-15(03)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel responsible for performing criticality analysis; system developer; organizational personnel with supply chain risk management responsibilities].
	SA-15(03)-Test	[SELECT FROM: Organizational processes for performing criticality analysis; mechanisms supporting and/or implementing criticality analysis].

SA-15(04)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | THREAT MODELING AND VULNERABILITY ANALYSIS
	[WITHDRAWN: Incorporated into SA-11(02).]

SA-15(05)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-15(05)_ODP	***thresholds to which attack surfaces are to be reduced are defined;***
	SA-15(05)	the developer of the system, system component, or system service is required to reduce attack surfaces to ***<SA-15(05)_ODP thresholds>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-15(05)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing development process, standards, and tools; procedures addressing attack surface reduction; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system or system service; system design documentation; network diagram; system configuration settings and associated documentation establishing/enforcing organization-defined thresholds for reducing attack surfaces; list of restricted ports, protocols, functions, and services; system security plan; other relevant documents or records].
	SA-15(05)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel responsible for attack surface reduction thresholds; system developer].
	SA-15(05)-Test	[SELECT FROM: Organizational processes for defining attack surface reduction thresholds].

SA-15(06)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CONTINUOUS IMPROVEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-15(06)	the developer of the system, system component, or system service is required to implement an explicit process to continuously improve the development process.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-15(06)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing development process, standards, and tools; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; quality goals and metrics for improving the system development process; security assessments; quality control reviews of system development process; plans of action and milestones for improving the system development process; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SA-15(06)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security and privacy responsibilities; system developer].

SA-15(07)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | AUTOMATED VULNERABILITY ANALYSIS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-15(07)_ODP[01]	***frequency at which to conduct vulnerability analysis is defined;***
	SA-15(07)_ODP[02]	***tools used to perform automated vulnerability analysis are defined;***
	SA-15(07)_ODP[03]	***personnel or roles to whom the outputs of tools and results of the analysis are to be delivered is/are defined;***
	SA-15(07)(a)	the developer of the system, system component, or system service is required to perform automated vulnerability analysis ***<SA-15(07)_ODP[01] frequency>*** using ***<SA-15(07)_ODP[02] tools>***;
	SA-15(07)(b)	the developer of the system, system component, or system service is required to determine the exploitation potential for discovered vulnerabilities ***<SA-15(07)_ODP[01] frequency>***;
	SA-15(07)(c)	the developer of the system, system component, or system service is required to determine potential risk mitigations ***<SA-15(07)_ODP[01] frequency>*** for delivered vulnerabilities;
	SA-15(07)(d)	the developer of the system, system component, or system service is required to deliver the outputs of the tools and results of the analysis ***<SA-15(07)_ODP[01] frequency>*** to ***<SA-15(07)_ODP[03] personnel or roles>***.

SA-15(07)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | AUTOMATED VULNERABILITY ANALYSIS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-15(07)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing development process, standards, and tools; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; vulnerability analysis tools and associated documentation; risk assessment reports; vulnerability analysis results; vulnerability mitigation reports; risk mitigation strategy documentation; system security plan; other relevant documents or records].
	SA-15(07)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; system developer; organizational personnel performing automated vulnerability analysis on the system].
	SA-15(07)-Test	[SELECT FROM: Organizational processes for vulnerability analysis of systems, system components, or system services under development; mechanisms supporting and/or implementing vulnerability analysis of systems, system components, or system services under development].

SA-15(08)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | REUSE OF THREAT AND VULNERABILITY INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-15(08)[01]	the developer of the system, system component, or system service is required to use threat modeling from similar systems, components, or services to inform the current development process;
	SA-15(08)[02]	the developer of the system, system component, or system service is required to use vulnerability analyses from similar systems, components, or services to inform the current development process.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-15(08)-Examine	[SELECT FROM: System and services acquisition policy; supply chain risk management plan; procedures addressing development process, standards, and tools; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; threat modeling and vulnerability analyses from similar systems, system components, or system services; system security plan; other relevant documents or records].
	SA-15(08)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; system developer; organizational personnel with supply chain risk management responsibilities].

SA-15(09)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | USE OF LIVE DATA
	[WITHDRAWN: Incorporated into SA-03(02).]

SA-15(10)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | INCIDENT RESPONSE PLAN	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-15(10)[01]	the developer of the system, system component, or system service is required to provide an incident response plan;
	SA-15(10)[02]	the developer of the system, system component, or system service is required to implement an incident response plan;
	SA-15(10)[03]	the developer of the system, system component, or system service is required to test an incident response plan.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-15(10)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing incident response, standards, and tools; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system components or services; acquisition documentation; solicitation documentation; service level agreements; developer incident response plan; system security plan; privacy plan; supply chain risk management plan; other relevant documents or records].
	SA-15(10)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; system developer; organizational personnel with supply chain risk management responsibilities].

SA-15(11)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ARCHIVE SYSTEM OR COMPONENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-15(11)	the developer of the system or system component is required to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security and privacy review.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-15(11)-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing development process, standards, and tools; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system or system component; evidence of archived system or component; system security plan; privacy plan; other relevant documents or records].
	SA-15(11)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; system developer; organizational personnel with privacy responsibilities].

SA-15(12)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-15(12)	the developer of the system or system component is required to minimize the use of personally identifiable information in development and test environments.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-15(12)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing the development process; procedures addressing the minimization of personally identifiable information in testing, training, and research; personally identifiable information processing policy; procedures addressing the authority to test with personally identifiable information; standards and tools; solicitation documentation; service level agreements; acquisition contracts for the system or services; system security plan; privacy plan; other relevant documents or records].
	SA-15(12)-Interview	[SELECT FROM: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities; system developer].
	SA-15(12)-Test	[SELECT FROM: Organizational processes for the minimization of personally identifiable information in development and test environments; mechanisms to facilitate the minimization of personally identifiable information in development and test environments].

SA-16	DEVELOPER-PROVIDED TRAINING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-16_ODP	***training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms provided by the developer of the system, system component, or system service is defined;***
	SA-16	the developer of the system, system component, or system service is required to provide ***<SA-16_ODP training>*** on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-16-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; procedures addressing developer-provided training; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; organizational security and privacy training policy; developer-provided training materials; training records; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SA-16-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security and privacy responsibilities; system developer; external or internal (in-house) developers with training responsibilities for the system, system component, or information system service].

SA-17	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-17(a)[01]	the developer of the system, system component, or system service is required to produce a design specification and security architecture that are consistent with the organization's security architecture, which is an integral part the organization's enterprise architecture;
	SA-17(a)[02]	the developer of the system, system component, or system service is required to produce a design specification and privacy architecture that are consistent with the organization's privacy architecture, which is an integral part the organization's enterprise architecture;
	SA-17(b)[01]	the developer of the system, system component, or system service is required to produce a design specification and security architecture that accurately and completely describe the required security functionality and the allocation of controls among physical and logical components;
	SA-17(b)[02]	the developer of the system, system component, or system service is required to produce a design specification and privacy architecture that accurately and completely describe the required privacy functionality and the allocation of controls among physical and logical components;
	SA-17(c)[01]	the developer of the system, system component, or system service is required to produce a design specification and security architecture that express how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection;
	SA-17(c)[02]	the developer of the system, system component, or system service is required to produce a design specification and privacy architecture that express how individual privacy functions, mechanisms, and services work together to provide required privacy capabilities and a unified approach to protection.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-17-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; enterprise architecture policy; enterprise architecture documentation; procedures addressing developer security and privacy architecture and design specifications for the system; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system design documentation; information system configuration settings and associated documentation; system security plan; privacy plan; other relevant documents or records].
	SA-17-Interview	[SELECT FROM: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities; system developer].

SA-17(01)	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | FORMAL POLICY MODEL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-17(01)_ODP[01]	***organizational security policy to be enforced is defined;***
	SA-17(01)_ODP[02]	***organizational privacy policy to be enforced is defined;***

SA-17(01)	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | FORMAL POLICY MODEL	
	SA-17(01)(a)[01]	as an integral part of the development process, the developer of the system, system component, or system service is required to produce a formal policy model describing the ***<SA-17(01)_ODP[01] organizational security policy>*** to be enforced;
	SA-17(01)(a)[02]	as an integral part of the development process, the developer of the system, system component, or system service is required to produce a formal policy model describing the ***<SA-17(01)_ODP[02] organizational privacy policy>*** to be enforced;
	SA-17(01)(b)[01]	the developer of the system, system component, or system service is required to prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security policy when implemented;
	SA-17(01)(b)[02]	the developer of the system, system component, or system service is required to prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational privacy policy when implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-17(01)-Examine	[SELECT FROM: System and services acquisition policy; system and services acquisition procedures; enterprise architecture policy; enterprise architecture documentation; procedures addressing developer security and privacy architecture and design specifications for the system; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system design documentation; system configuration settings and associated documentation; system security plan; privacy plan; other relevant documents or records].
	SA-17(01)-Interview	[SELECT FROM: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities; system developer].

SA-17(02)	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | SECURITY-RELEVANT COMPONENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-17(02)(a)[01]	the developer of the system, system component, or system service is required to define security-relevant hardware;
	SA-17(02)(a)[02]	the developer of the system, system component, or system service is required to define security-relevant software;
	SA-17(02)(a)[03]	the developer of the system, system component, or system service is required to define security-relevant firmware;
	SA-17(02)(b)	the developer of the system, system component, or system service is required to provide a rationale that the definition for security-relevant hardware, software, and firmware is complete.

SA-17(02)	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | SECURITY-RELEVANT COMPONENTS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-17(02)-Examine	[SELECT FROM: System and services acquisition policy; enterprise architecture policy; procedures addressing developer security architecture and design specifications for the system; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; list of security-relevant hardware, software, and firmware components; documented rationale of completeness regarding definitions provided for security-relevant hardware, software, and firmware; system security plan; other relevant documents or records].
	SA-17(02)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; system developers; organizational personnel with information security architecture and design responsibilities].

SA-17(03)	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | FORMAL CORRESPONDENCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-17(03)(a)[01]	as an integral part of the development process, the developer of the system, system component, or system service is required to produce a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions;
	SA-17(03)(a)[02]	as an integral part of the development process, the developer of the system, system component, or system service is required to produce a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of error messages;
	SA-17(03)(a)[03]	as an integral part of the development process, the developer of the system, system component, or system service is required to produce a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of effects;
	SA-17(03)(b)	the developer of the system, system component, or system service is required to show proof that the formal top-level specification is consistent with the formal policy model to the extent feasible with additional informal demonstration as necessary;
	SA-17(03)(c)	the developer of the system, system component, or system service is required to show via informal demonstration that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;
	SA-17(03)(d)	the developer of the system, system component, or system service is required to show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and firmware;
	SA-17(03)(e)	the developer of the system, system component, or system service is required to describe the security-relevant hardware, software, and firmware mechanisms that are not addressed in the formal top-level specification but are strictly internal to the security-relevant hardware, software, and firmware.

SA-17(03)	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | FORMAL CORRESPONDENCE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-17(03)-Examine	[SELECT FROM: System and services acquisition policy; enterprise architecture policy; formal policy model; procedures addressing developer security architecture and design specifications for the system; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; formal top-level specification documentation; system security architecture and design documentation; system design documentation; system configuration settings and associated documentation; documentation describing security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification documentation; system security plan; other relevant documents or records].
	SA-17(03)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; system developer; organizational personnel with information security architecture and design responsibilities].

SA-17(04)	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | INFORMAL CORRESPONDENCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-17(04)_ODP	***one of the following PARAMETER VALUES is selected: {informal demonstration, convincing argument with formal methods as feasible};***
	SA-17(04)(a)[01]	as an integral part of the development process, the developer of the system, system component, or system service is required to produce an informal, descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions;
	SA-17(04)(a)[02]	as an integral part of the development process, the developer of the system, system component, or system service is required to produce an informal, descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of error messages;
	SA-17(04)(a)[03]	as an integral part of the development process, the developer of the system, system component, or system service is required to produce an informal, descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of effects;
	SA-17(04)(b)	the developer of the system, system component, or system service is required to show via ***<SA-17(04)_ODP SELECTED PARAMETER VALUE>*** that the descriptive top-level specification is consistent with the formal policy model;
	SA-17(04)(c)	the developer of the system, system component, or system service is required to show via informal demonstration that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;
	SA-17(04)(d)	the developer of the system, system component, or system service is required to show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware;

SA-17(04)	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | INFORMAL CORRESPONDENCE	
	SA-17(04)(e)	the developer of the system, system component, or system service is required to describe the security-relevant hardware, software, and firmware mechanisms that are not addressed in the descriptive top-level specification but are strictly internal to the security-relevant hardware, software, and firmware.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-17(04)-Examine	[SELECT FROM: System and services acquisition policy; enterprise architecture policy; formal policy model; procedures addressing developer security architecture and design specifications for the system; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; informal, descriptive top-level specification documentation; system security architecture and design documentation; system design documentation; system configuration settings and associated documentation; documentation describing security-relevant hardware, software, and firmware mechanisms not addressed in the informal, descriptive top-level specification documentation; system security plan; other relevant documents or records].
	SA-17(04)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; system developer; organizational personnel with information security architecture and design responsibilities].

SA-17(05)	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | CONCEPTUALLY SIMPLE DESIGN	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-17(05)(a)	the developer of the system, system component, or system service is required to design and structure the security-relevant hardware, software, and firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics;
	SA-17(05)(b)	the developer of the system, system component, or system service is required to internally structure the security-relevant hardware, software, and firmware with specific regard for this mechanism.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-17(05)-Examine	[SELECT FROM: System and services acquisition policy; enterprise architecture policy; procedures addressing developer security architecture and design specifications for the system; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system design documentation; system security architecture documentation; system configuration settings and associated documentation; developer documentation describing the design and structure of security-relevant hardware, software, and firmware components; system security plan; other relevant documents or records].

SA-17(05)	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | CONCEPTUALLY SIMPLE DESIGN	
	SA-17(05)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; system developer; organizational personnel with information security architecture and design responsibilities].

SA-17(06)	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | STRUCTURE FOR TESTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-17(06)	the developer of the system, system component, or system service is required to structure security-relevant hardware, software, and firmware to facilitate testing.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-17(06)-Examine	[SELECT FROM: System and services acquisition policy; enterprise architecture policy; procedures addressing developer security architecture and design specifications for the system; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system design documentation; system security architecture documentation; privacy architecture documentation; system configuration settings and associated documentation; developer documentation describing the design and structure of security-relevant hardware, software, and firmware components to facilitate testing; system security plan; privacy plan; other relevant documents or records].
	SA-17(06)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security and privacy responsibilities; system developer; organizational personnel with information security and privacy architecture and design responsibilities].

SA-17(07)	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | STRUCTURE FOR LEAST PRIVILEGE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-17(07)	the developer of the system, system component, or system service is required to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.

SA-17(07)	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | STRUCTURE FOR LEAST PRIVILEGE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-17(07)-Examine	[SELECT FROM: System and services acquisition policy; enterprise architecture policy; procedures addressing developer security architecture and design specifications for the system; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system design documentation; system security architecture documentation; system configuration settings and associated documentation; developer documentation describing the design and structure of security-relevant hardware, software, and firmware components to facilitate controlling access with least privilege; system security plan; other relevant documents or records].
	SA-17(07)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; system developer; organizational personnel with information security architecture and design responsibilities].

SA-17(08)	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | ORCHESTRATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-17(08)_ODP[01]	***critical systems or system components are defined;***
	SA-17(08)_ODP[02]	***capabilities to be implemented by systems or components are defined;***
	SA-17(08)	***<SA-17(08)_ODP[01] critical systems>*** are designed with coordinated behavior to implement ***<SA-17(08)_ODP[02] capabilities>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-17(08)-Examine	[SELECT FROM: System and services acquisition policy; enterprise architecture policy; procedures addressing developer security and privacy architecture and design; enterprise architecture; security architecture; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system design documentation; system configuration settings and associated documentation; developer documentation describing design orchestration; system security plan; privacy plan; other relevant documents or records].
	SA-17(08)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security and privacy responsibilities; system developer; organizational personnel with information security architecture responsibilities].

SA-17(09)	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | DESIGN DIVERSITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-17(09)_ODP	***critical systems or system components to be designed differently are defined;***

SA-17(09)	DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN | DESIGN DIVERSITY	
	SA-17(09)	different designs are used for ***<SA-17(09)_ODP critical systems>*** to satisfy a common set of requirements or to provide equivalent functionality.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-17(09)-Examine	[SELECT FROM: System and services acquisition policy; enterprise architecture policy; procedures addressing developer security architecture and design diversity for the system; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system design documentation; system security architecture documentation; system configuration settings and associated documentation; developer documentation describing design diversity; system security plan; other relevant documents or records].
	SA-17(09)-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; system developer; organizational personnel with information security architecture responsibilities].

SA-18	TAMPER RESISTANCE AND DETECTION
	[WITHDRAWN: Moved to SR-09.]

SA-18(01)	TAMPER RESISTANCE AND DETECTION | MULTIPLE PHASES OF SYSTEM DEVELOPMENT LIFE CYCLE
	[WITHDRAWN: Moved to SR-09(01).]

SA-18(02)	TAMPER RESISTANCE AND DETECTION | INSPECTION OF SYSTEMS OR COMPONENTS
	[WITHDRAWN: Moved to SR-10.]

SA-19	COMPONENT AUTHENTICITY
	[WITHDRAWN: Moved to SR-11.]

SA-19(01)	COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING
	[WITHDRAWN: Moved to SR-11(01).]

SA-19(02)	COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR
	[WITHDRAWN: Moved to SR-11(02).]

SA-19(03)	COMPONENT AUTHENTICITY | COMPONENT DISPOSAL
	[WITHDRAWN: Moved to SR-12.]

SA-19(04)	COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT SCANNING
	[WITHDRAWN: Moved to SR-11(03).]

SA-20	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-20_ODP	***critical system components to be reimplemented or custom-developed are defined;***
	SA-20	***<SA-20_ODP critical system>*** are reimplemented or custom-developed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-20-Examine	[SELECT FROM: Supply chain risk management plan; system and services acquisition policy; procedures addressing the customized development of critical system components; system design documentation; system configuration settings and associated documentation; system development life cycle documentation addressing the custom development of critical system components; configuration management records; system audit records; system security plan; other relevant documents or records].
	SA-20-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with responsibility for the reimplementation or customized development of critical system components].
	SA-20-Test	[SELECT FROM: Organizational processes for the reimplementation or customized development of critical system components; mechanisms supporting and/or implementing the reimplementation or customized development of critical system components].

SA-21	DEVELOPER SCREENING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-21_ODP[01]	***the system, systems component, or system service that the developer has access to is/are defined;***
	SA-21_ODP[02]	***official government duties assigned to the developer are defined;***
	SA-21_ODP[03]	***additional personnel screening criteria for the developer are defined;***
	SA-21a.	the developer of ***<SA-21_ODP[01] system, systems component, or system service>*** is required to have appropriate access authorizations as determined by assigned ***<SA-21_ODP[02] official government duties>***;
	SA-21b.	the developer of ***<SA-21_ODP[01] system, systems component, or system service>*** is required to satisfy ***<SA-21_ODP[03] additional personnel screening criteria>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-21-Examine	[SELECT FROM: System and services acquisition policy; personnel security policy and procedures; procedures addressing personnel screening; system design documentation; acquisition documentation; service level agreements; acquisition contracts for developer services; system configuration settings and associated documentation; list of appropriate access authorizations required by the developers of the system; personnel screening criteria and associated documentation; system security plan; supply chain risk management plan; other relevant documents or records].
	SA-21-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel responsible for developer screening].
	SA-21-Test	[SELECT FROM: Organizational processes for developer screening; mechanisms supporting developer screening].

SA-21(01)	DEVELOPER SCREENING | VALIDATION OF SCREENING
	[WITHDRAWN: Incorporated into SA-21.]

SA-22	UNSUPPORTED SYSTEM COMPONENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-22_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {in-house support; <SA-22_ODP[02] support from external providers>};***
	SA-22_ODP[02]	***support from external providers is defined (if selected);***
	SA-22a.	system components are replaced when support for the components is no longer available from the developer, vendor, or manufacturer;
	SA-22b.	***<SA-22_ODP[01] SELECTED PARAMETER VALUE(S)>*** provide options for alternative sources for continued support for unsupported components.

SA-22	UNSUPPORTED SYSTEM COMPONENTS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-22-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing the replacement or continued use of unsupported system components; documented evidence of replacing unsupported system components; documented approvals (including justification) for the continued use of unsupported system components; system security plan; supply chain risk management plan; other relevant documents or records].
	SA-22-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with the responsibility for the system development life cycle; organizational personnel responsible for component replacement].
	SA-22-Test	[SELECT FROM: Organizational processes for replacing unsupported system components; mechanisms supporting and/or implementing the replacement of unsupported system components].

SA-22(01)	UNSUPPORTED SYSTEM COMPONENTS | ALTERNATIVE SOURCES FOR CONTINUED SUPPORT
	[WITHDRAWN: Incorporated into SA-22.]

SA-23	SPECIALIZATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SA-23_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {design modification; augmentation; reconfiguration};***
	SA-23_ODP[02]	***systems or system components supporting mission-essential services or functions are defined;***
	SA-23	***<SA-23_ODP[01] SELECTED PARAMETER VALUE(S)>*** is employed on ***<SA-23_ODP[02] systems or system components>*** supporting essential services or functions to increase the trustworthiness in those systems or components.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SA-23-Examine	[SELECT FROM: System and services acquisition policy; procedures addressing design modification, augmentation, or reconfiguration of systems or system components; documented evidence of design modification, augmentation, or reconfiguration; system security plan; supply chain risk management plan; other relevant documents or records].
	SA-23-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with the responsibility for security architecture; organizational personnel responsible for configuration management].

SA-23	SPECIALIZATION	
	SA-23-Test	[SELECT FROM: Organizational processes for the modification of design, augmentation, or reconfiguration of systems or system components; mechanisms supporting and/or implementing design modification, augmentation, or reconfiguration of systems or system components].

4.18 SYSTEM AND COMMUNICATIONS PROTECTION

SC-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-01_ODP[01]	***personnel or roles to whom the system and communications protection policy is to be disseminated is/are defined;***
	SC-01_ODP[02]	***personnel or roles to whom the system and communications protection procedures are to be disseminated is/are defined;***
	SC-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business-process-level; system-level};***
	SC-01_ODP[04]	***an official to manage the system and communications protection policy and procedures is defined;***
	SC-01_ODP[05]	***the frequency at which the current system and communications protection policy is reviewed and updated is defined;***
	SC-01_ODP[06]	***events that would require the current system and communications protection policy to be reviewed and updated are defined;***
	SC-01_ODP[07]	***the frequency at which the current system and communications protection procedures are reviewed and updated is defined;***
	SC-01_ODP[08]	***events that would require the system and communications protection procedures to be reviewed and updated are defined;***
	SC-01a.[01]	a system and communications protection policy is developed and documented;
	SC-01a.[02]	the system and communications protection policy is disseminated to ***<SC-01_ODP[01] personnel or roles>***;
	SC-01a.[03]	system and communications protection procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls are developed and documented;
	SC-01a.[04]	the system and communications protection procedures are disseminated to ***<SC-01_ODP[02] personnel or roles>***;
	SC-01a.01(a)[01]	the ***<SC-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and communications protection policy addresses purpose;
	SC-01a.01(a)[02]	the ***<SC-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and communications protection policy addresses scope;
	SC-01a.01(a)[03]	the ***<SC-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and communications protection policy addresses roles;
	SC-01a.01(a)[04]	the ***<SC-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and communications protection policy addresses responsibilities;
	SC-01a.01(a)[05]	the ***<SC-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and communications protection policy addresses management commitment;
	SC-01a.01(a)[06]	the ***<SC-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and communications protection policy addresses coordination among organizational entities;

SC-01	POLICY AND PROCEDURES	
	SC-01a.01(a)[07]	the ***<SC-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and communications protection policy addresses compliance;
	SC-01a.01(b)	the ***<SC-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and communications protection policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines;
	SC-01b.	the ***<SC-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the system and communications protection policy and procedures;
	SC-01c.01[01]	the current system and communications protection policy is reviewed and updated ***<SC-01_ODP[05] frequency>***;
	SC-01c.01[02]	the current system and communications protection policy is reviewed and updated following ***<SC-01_ODP[06] events>***;
	SC-01c.02[01]	the current system and communications protection procedures are reviewed and updated ***<SC-01_ODP[07] frequency>***;
	SC-01c.02[02]	the current system and communications protection procedures are reviewed and updated following ***<SC-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-01-Examine	[SELECT FROM: System and communications protection policy; system and communications protection procedures; system security plan; privacy plan; risk management strategy documentation; audit findings; other relevant documents or records].
	SC-01-Interview	[SELECT FROM: Organizational personnel with system and communications protection responsibilities; organizational personnel with information security and privacy responsibilities].

SC-02	SEPARATION OF SYSTEM AND USER FUNCTIONALITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-02	user functionality, including user interface services, is separated from system management functionality.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-02-Examine	[SELECT FROM: System and communications protection policy; procedures addressing application partitioning; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-02-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].
	SC-02-Test	[SELECT FROM: Separation of user functionality from system management functionality].

SC-02(01)	SEPARATION OF SYSTEM AND USER FUNCTIONALITY | INTERFACES FOR NON-PRIVILEGED USERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-02(01)	the presentation of system management functionality is prevented at interfaces to non-privileged users.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-02(01)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing application partitioning; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-02(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; non-privileged users of the system; system developer].
	SC-02(01)-Test	[SELECT FROM: Separation of user functionality from system management functionality].

SC-02(02)	SEPARATION OF SYSTEM AND USER FUNCTIONALITY | DISASSOCIABILITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-02(02)	state information is stored separately from applications and software.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-02(02)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing application and software partitioning; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; other relevant documents or records].
	SC-02(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; system developer].
	SC-02(02)-Test	[SELECT FROM: Separation of application state information from software].

SC-03	SECURITY FUNCTION ISOLATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-03	security functions are isolated from non-security functions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-03-Examine	[SELECT FROM: System and communications protection policy; procedures addressing security function isolation; list of security functions to be isolated from non-security functions; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].

SC-03	SECURITY FUNCTION ISOLATION	
	SC-03-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].
	SC-03-Test	[SELECT FROM: Separation of security functions from non-security functions within the system].

SC-03(01)	SECURITY FUNCTION ISOLATION | HARDWARE SEPARATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-03(01)	hardware separation mechanisms are employed to implement security function isolation.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-03(01)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing security function isolation; system design documentation; hardware separation mechanisms; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-03(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].
	SC-03(01)-Test	[SELECT FROM: Separation of security functions from non-security functions within the system].

SC-03(02)	SECURITY FUNCTION ISOLATION | ACCESS AND FLOW CONTROL FUNCTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-03(02)[01]	security functions enforcing access control are isolated from non-security functions;
	SC-03(02)[02]	security functions enforcing access control are isolated from other security functions;
	SC-03(02)[03]	security functions enforcing information flow control are isolated from non-security functions;
	SC-03(02)[04]	security functions enforcing information flow control are isolated from other security functions.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-03(02)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing security function isolation; list of critical security functions; system design documentation; system configuration settings and associated documentation; system audit records system security plan; other relevant documents or records].
	SC-03(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].

SC-03(02)	SECURITY FUNCTION ISOLATION | ACCESS AND FLOW CONTROL FUNCTIONS	
	SC-03(02)-Test	[SELECT FROM: Isolation of security functions enforcing access and information flow control].

SC-03(03)	SECURITY FUNCTION ISOLATION | MINIMIZE NONSECURITY FUNCTIONALITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-03(03)	the number of non-security functions included within the isolation boundary containing security functions is minimized.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-03(03)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing security function isolation; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-03(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	SC-03(03)-Test	[SELECT FROM: Mechanisms supporting and/or implementing an isolation boundary].

SC-03(04)	SECURITY FUNCTION ISOLATION | MODULE COUPLING AND COHESIVENESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-03(04)[01]	security functions are implemented as largely independent modules that maximize internal cohesiveness within modules;
	SC-03(04)[02]	security functions are implemented as largely independent modules that minimize coupling between modules.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-03(04)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing security function isolation; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-03(04)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	SC-03(04)-Test	[SELECT FROM: Organizational processes for maximizing internal cohesiveness within modules and minimizing coupling between modules; mechanisms supporting and/or implementing security functions as independent modules].

SC-03(05)	SECURITY FUNCTION ISOLATION | LAYERED STRUCTURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-03(05)	security functions are implemented as a layered structure, minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-03(05)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing security function isolation; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-03(05)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	SC-03(05)-Test	[SELECT FROM: Organizational processes for implementing security functions as a layered structure that minimizes interactions between layers and avoids dependence by lower layers on functionality/correctness of higher layers; mechanisms supporting and/or implementing security functions as a layered structure].

SC-04	INFORMATION IN SHARED SYSTEM RESOURCES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-04[01]	unauthorized information transfer via shared system resources is prevented;
	SC-04[02]	unintended information transfer via shared system resources is prevented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-04-Examine	[SELECT FROM: System and communications protection policy; procedures addressing information protection in shared system resources; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-04-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].
	SC-04-Test	[SELECT FROM: Mechanisms preventing the unauthorized and unintended transfer of information via shared system resources].

SC-04(01)	INFORMATION IN SHARED SYSTEM RESOURCES | SECURITY LEVELS
	[WITHDRAWN: Incorporated into SC-04.]

SC-04(02)	INFORMATION IN SHARED SYSTEM RESOURCES | MULTILEVEL OR PERIODS PROCESSING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-04(02)_ODP	***procedures to prevent unauthorized information transfer via shared resources are defined;***
	SC-04(02)	unauthorized information transfer via shared resources is prevented in accordance with ***<SC-04(02)_ODP procedures>*** when system processing explicitly switches between different information classification levels or security categories.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-04(02)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing information protection in shared system resources; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-04(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].
	SC-04(02)-Test	[SELECT FROM: Mechanisms preventing the unauthorized transfer of information via shared system resources].

SC-05	DENIAL-OF-SERVICE PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-05_ODP[01]	***types of denial-of-service events to be protected against or limited are defined;***
	SC-05_ODP[02]	***one of the following PARAMETER VALUES is selected: {protect against; limit};***
	SC-05_ODP[03]	***controls to achieve the denial-of-service objective by type of denial-of-service event are defined;***
	SC-05a.	the effects of ***<SC-05_ODP[01] types of denial-of-service events>*** are ***<SC-05_ODP[02] SELECTED PARAMETER VALUE>***;
	SC-05b.	***<SC-05_ODP[03] controls by type of denial-of-service event>*** are employed to achieve the denial-of-service protection objective.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-05-Examine	[SELECT FROM: System and communications protection policy; procedures addressing denial-of-service protection; system design documentation; list of denial-of-service attacks requiring employment of security safeguards to protect against or limit effects of such attacks; list of security safeguards protecting against or limiting the effects of denial-of-service attacks; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-05-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with incident response responsibilities; system developer].
	SC-05-Test	[SELECT FROM: Mechanisms protecting against or limiting the effects of denial-of-service attacks].

SC-05(01)	DENIAL-OF-SERVICE PROTECTION | RESTRICT ABILITY TO ATTACK OTHER SYSTEMS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-05(01)_ODP	***denial-of-service attacks for which to restrict the ability of individuals to launch are defined;***
	SC-05(01)	the ability of individuals to launch ***<SC-05(01)_ODP denial-of-service attacks>*** against other systems is restricted.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-05(01)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing denial-of-service protection; system design documentation; list of denial-of-service attacks launched by individuals against systems; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-05(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with incident response responsibilities; system developer].
	SC-05(01)-Test	[SELECT FROM: Mechanisms restricting the ability to launch denial-of-service attacks against other systems].

SC-05(02)	DENIAL-OF-SERVICE PROTECTION | CAPACITY, BANDWIDTH, AND REDUNDANCY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-05(02)	capacity, bandwidth, or other redundancies to limit the effects of information flooding denial-of-service attacks are managed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-05(02)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing denial-of-service protection; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-05(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with incident response responsibilities; system developer].
	SC-05(02)-Test	[SELECT FROM: Mechanisms implementing the management of system bandwidth, capacity, and redundancy to limit the effects of information flooding denial-of-service attacks].

SC-05(03)	DENIAL-OF-SERVICE PROTECTION | DETECTION AND MONITORING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-05(03)_ODP[01]	***monitoring tools for detecting indicators of denial-of-service attacks are defined;***

SC-05(03)	DENIAL-OF-SERVICE PROTECTION | DETECTION AND MONITORING	
	SC-05(03)_ODP[02]	***system resources to be monitored to determine if sufficient resources exist to prevent effective denial-of-service attacks are defined;***
	SC-05(03)(a)	***<SC-05(03)_ODP[01] monitoring tools>*** are employed to detect indicators of denial-of-service attacks against or launched from the system;
	SC-05(03)(b)	***<SC-05(03)_ODP[02] system resources>*** are monitored to determine if sufficient resources exist to prevent effective denial-of-service attacks.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-05(03)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing denial-of-service protection; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-05(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with detection and monitoring responsibilities].
	SC-05(03)-Test	[SELECT FROM: Mechanisms/tools implementing system monitoring for denial-of-service attacks].

SC-06	RESOURCE AVAILABILITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-06_ODP[01]	***resources to be allocated to protect the availability of resources are defined;***
	SC-06_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {priority; quota; <SC-06_ODP[03] controls>};***
	SC-06_ODP[03]	***controls to protect the availability of resources are defined (if selected);***
	SC-06	the availability of resources is protected by allocating ***<SC-06_ODP[01] resources>*** by ***<SC-06_ODP[02] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-06-Examine	[SELECT FROM: System and communications protection policy; procedures addressing prioritization of system resources; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-06-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].
	SC-06-Test	[SELECT FROM: Mechanisms supporting and/or implementing a resource allocation capability; safeguards employed to protect availability of resources].

SC-07	BOUNDARY PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07_ODP	***one of the following PARAMETER VALUES is selected: {physically; logically};***
	SC-07a.[01]	communications at external managed interfaces to the system are monitored;
	SC-07a.[02]	communications at external managed interfaces to the system are controlled;
	SC-07a.[03]	communications at key internal managed interfaces within the system are monitored;
	SC-07a.[04]	communications at key internal managed interfaces within the system are controlled;
	SC-07b.	subnetworks for publicly accessible system components are ***<SC-07_ODP SELECTED PARAMETER VALUE>*** separated from internal organizational networks;
	SC-07c.	external networks or systems are only connected to through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the system; system design documentation; boundary protection hardware and software; system configuration settings and associated documentation; enterprise security architecture documentation; system audit records; system security plan; other relevant documents or records].
	SC-07-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].
	SC-07-Test	[SELECT FROM: Mechanisms implementing boundary protection capabilities].

SC-07(01)	BOUNDARY PROTECTION | PHYSICALLY SEPARATED SUBNETWORKS
	[WITHDRAWN: Incorporated into SC-07.]

SC-07(02)	BOUNDARY PROTECTION | PUBLIC ACCESS
	[WITHDRAWN: Incorporated into SC-07.]

SC-07(03)	BOUNDARY PROTECTION | ACCESS POINTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(03)	the number of external network connections to the system is limited.

SC-07(03)	BOUNDARY PROTECTION | ACCESS POINTS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(03)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; boundary protection hardware and software; system architecture and configuration documentation; system configuration settings and associated documentation; communications and network traffic monitoring logs; system audit records; system security plan; other relevant documents or records].
	SC-07(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities].
	SC-07(03)-Test	[SELECT FROM: Mechanisms implementing boundary protection capabilities; mechanisms limiting the number of external network connections to the system].

SC-07(04)	BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(04)_ODP	***the frequency at which to review exceptions to traffic flow policy is defined;***
	SC-07(04)(a)	a managed interface is implemented for each external telecommunication service;
	SC-07(04)(b)	a traffic flow policy is established for each managed interface;
	SC-07(04)(c)[01]	the confidentiality of the information being transmitted across each interface is protected;
	SC-07(04)(c)[02]	the integrity of the information being transmitted across each interface is protected;
	SC-07(04)(d)	each exception to the traffic flow policy is documented with a supporting mission or business need and duration of that need;
	SC-07(04)(e)[01]	exceptions to the traffic flow policy are reviewed ***<SC-07(04)_ODP frequency>***;
	SC-07(04)(e)[02]	exceptions to the traffic flow policy that are no longer supported by an explicit mission or business need are removed;
	SC-07(04)(f)	unauthorized exchanges of control plan traffic with external networks are prevented;
	SC-07(04)(g)	information is published to enable remote networks to detect unauthorized control plane traffic from internal networks;
	SC-07(04)(h)	unauthorized control plane traffic is filtered from external networks.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(04)-Examine	[SELECT FROM: System and communications protection policy; traffic flow policy; information flow control policy; procedures addressing boundary protection; system security architecture; system design documentation; boundary protection hardware and software; system architecture and configuration documentation; system configuration settings and associated documentation; records of traffic flow policy exceptions; system audit records; system security plan; other relevant documents or records].

SC-07(04)	BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES	
	SC-07(04)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities].
	SC-07(04)-Test	[SELECT FROM: Organizational processes for documenting and reviewing exceptions to the traffic flow policy; organizational processes for removing exceptions to the traffic flow policy; mechanisms implementing boundary protection capabilities; managed interfaces implementing traffic flow policy].

SC-07(05)	BOUNDARY PROTECTION | DENY BY DEFAULT — ALLOW BY EXCEPTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(05)_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {at managed interfaces; for <SC-07(05)_ODP[02] systems>};***
	SC-07(05)_ODP[02]	***systems for which network communications traffic is denied by default and network communications traffic is allowed by exception are defined (if selected).***
	SC-07(05)[01]	network communications traffic is denied by default ***<SC-07(05)_ODP[01] SELECTED PARAMETER VALUE(S)>***;
	SC-07(05)[02]	network communications traffic is allowed by exception ***<SC-07(05)_ODP[01] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(05)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-07(05)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].
	SC-07(05)-Test	[SELECT FROM: Mechanisms implementing traffic management at managed interfaces].

SC-07(06)	BOUNDARY PROTECTION | RESPONSE TO RECOGNIZED FAILURES
	[WITHDRAWN: Incorporated into SC-07(18).]

SC-07(07)	BOUNDARY PROTECTION | SPLIT TUNNELING FOR REMOTE DEVICES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(07)_ODP	***safeguards to securely provision split tunneling are defined;***

SC-07(07)	BOUNDARY PROTECTION | SPLIT TUNNELING FOR REMOTE DEVICES	
	SC-07(07)	split tunneling is prevented for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using ***<SC-07(07)_ODP safeguards>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(07)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-07(07)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].
	SC-07(07)-Test	[SELECT FROM: Mechanisms implementing boundary protection capabilities; mechanisms supporting/restricting non-remote connections].

SC-07(08)	BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(08)_ODP[01]	***internal communications traffic to be routed to external networks is defined;***
	SC-07(08)_ODP[02]	***external networks to which internal communications traffic is to be routed are defined;***
	SC-07(08)	***<SC-07(08)_ODP[01] internal communications traffic>*** is routed to ***<SC-07(08)_ODP[02] external networks>*** through authenticated proxy servers at managed interfaces.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(08)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-07(08)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].
	SC-07(08)-Test	[SELECT FROM: Mechanisms implementing traffic management through authenticated proxy servers at managed interfaces].

SC-07(09)	BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(09)(a)[01]	outgoing communications traffic posing a threat to external systems is detected;
	SC-07(09)(a)[02]	outgoing communications traffic posing a threat to external systems is denied;
	SC-07(09)(b)	the identity of internal users associated with denied communications is audited.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(09)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-07(09)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].
	SC-07(09)-Test	[SELECT FROM: Mechanisms implementing boundary protection capabilities; mechanisms implementing the detection and denial of threatening outgoing communications traffic; mechanisms implementing auditing of outgoing communications traffic].

SC-07(10)	BOUNDARY PROTECTION | PREVENT EXFILTRATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(10)_ODP	***the frequency for conducting exfiltration tests is defined;***
	SC-07(10)(a)	the exfiltration of information is prevented;
	SC-07(10)(b)	exfiltration tests are conducted ***<SC-07(10)_ODP frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(10)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-07(10)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities].
	SC-07(10)-Test	[SELECT FROM: Mechanisms implementing boundary protection capabilities that prevent the unauthorized exfiltration of information across managed interfaces].

SC-07(11)	BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(11)_ODP[01]	***authorized sources of incoming communications to be routed are defined;***
	SC-07(11)_ODP[02]	***authorized destinations to which incoming communications from authorized sources may be routed are defined;***
	SC-07(11)	only incoming communications from ***<SC-07(11)_ODP[01] authorized sources>*** are allowed to be routed to ***<SC-07(11)_ODP[02] authorized destinations>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(11)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-07(11)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].
	SC-07(11)-Test	[SELECT FROM: Mechanisms implementing boundary protection capabilities with respect to source/destination address pairs].

SC-07(12)	BOUNDARY PROTECTION | HOST-BASED PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(12)_ODP[01]	***host-based boundary protection mechanisms to be implemented are defined;***
	SC-07(12)_ODP[02]	***system components where host-based boundary protection mechanisms are to be implemented are defined;***
	SC-07(12)	***<SC-07(12)_ODP[01] host-based boundary protection mechanisms>*** are implemented at ***<SC-07(12)_ODP[02] system components>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(12)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; boundary protection hardware and software; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-07(12)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities; system users].
	SC-07(12)-Test	[SELECT FROM: Mechanisms implementing host-based boundary protection capabilities].

SC-07(13)	BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(13)_ODP	***information security tools, mechanisms, and support components to be isolated from other internal system components are defined;***
	SC-07(13)	***<SC-07(13)_ODP information security tools, mechanisms, and support components>*** are isolated from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(13)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; list of security tools and support components to be isolated from other internal system components; system audit records; system security plan; other relevant documents or records].
	SC-07(13)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities].
	SC-07(13)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the isolation of information security tools, mechanisms, and support components].

SC-07(14)	BOUNDARY PROTECTION | PROTECT AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(14)_ODP	***managed interfaces to be protected against unauthorized physical connections are defined;***
	SC-07(14)	***<SC-07(14)_ODP managed interfaces>*** are protected against unauthorized physical connections.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(14)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; facility communications and wiring diagram system security plan; other relevant documents or records].
	SC-07(14)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities].
	SC-07(14)-Test	[SELECT FROM: Mechanisms supporting and/or implementing protection against unauthorized physical connections].

SC-07(15)	BOUNDARY PROTECTION | NETWORKED PRIVILEGED ACCESSES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(15)[01]	networked, privileged accesses are routed through a dedicated, managed interface for purposes of access control;
	SC-07(15)[02]	networked, privileged accesses are routed through a dedicated, managed interface for purposes of auditing.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(15)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; audit logs; system security plan; other relevant documents or records].
	SC-07(15)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].
	SC-07(15)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the routing of networked, privileged access through dedicated, managed interfaces].

SC-07(16)	BOUNDARY PROTECTION | PREVENT DISCOVERY OF SYSTEM COMPONENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(16)	the discovery of specific system components that represent a managed interface is prevented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(16)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-07(16)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].
	SC-07(16)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the prevention of discovery of system components at managed interfaces].

SC-07(17)	BOUNDARY PROTECTION | AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(17)	adherence to protocol formats is enforced.

SC-07(17)	BOUNDARY PROTECTION | AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(17)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system architecture; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-07(17)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].
	SC-07(17)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the enforcement of adherence to protocol formats].

SC-07(18)	BOUNDARY PROTECTION | FAIL SECURE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(18)	systems are prevented from entering unsecure states in the event of an operational failure of a boundary protection device.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(18)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system architecture; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-07(18)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].
	SC-07(18)-Test	[SELECT FROM: Mechanisms supporting and/or implementing secure failure].

SC-07(19)	BOUNDARY PROTECTION | BLOCK COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(19)_ODP	***communication clients that are independently configured by end users and external service providers are defined;***
	SC-07(19)[01]	inbound communications traffic is blocked between ***<SC-07(19)_ODP communication clients>*** that are independently configured by end users and external service providers;
	SC-07(19)[02]	outbound communications traffic is blocked between ***<SC-07(19)_ODP communication clients>*** that are independently configured by end users and external service providers.

SC-07(19)	BOUNDARY PROTECTION | BLOCK COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(19)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; list of communication clients independently configured by end users and external service providers; system audit records; system security plan; other relevant documents or records].
	SC-07(19)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities].
	SC-07(19)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the blocking of inbound and outbound communications traffic between communication clients independently configured by end users and external service providers].

SC-07(20)	BOUNDARY PROTECTION | DYNAMIC ISOLATION AND SEGREGATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(20)_ODP	***system components to be dynamically isolated from other system components are defined;***
	SC-07(20)	the capability to dynamically isolate ***<SC-07(20)_ODP system components>*** from other system components is provided.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(20)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; list of system components to be dynamically isolated/segregated from other components of the system; system audit records; system security plan; other relevant documents or records].
	SC-07(20)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].
	SC-07(20)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the capability to dynamically isolate/segregate system components].

SC-07(21)	BOUNDARY PROTECTION | ISOLATION OF SYSTEM COMPONENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(21)_ODP[01]	***system components to be isolated by boundary protection mechanisms are defined;***

SC-07(21)	BOUNDARY PROTECTION | ISOLATION OF SYSTEM COMPONENTS	
	SC-07(21)_ODP[02]	***missions and/or business functions to be supported by system components isolated by boundary protection mechanisms are defined;***
	SC-07(21)	boundary protection mechanisms are employed to isolate ***<SC-07(21)_ODP[01] system components>*** supporting ***<SC-07(21)_ODP[02] missions and/or business functions>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(21)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; enterprise architecture documentation; system architecture; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-07(21)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with boundary protection responsibilities].
	SC-07(21)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the capability to separate system components supporting organizational missions and/or business functions].

SC-07(22)	BOUNDARY PROTECTION | SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(22)	separate network addresses are implemented to connect to systems in different security domains.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(22)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-07(22)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].
	SC-07(22)-Test	[SELECT FROM: Mechanisms supporting and/or implementing separate network addresses/different subnets].

SC-07(23)	BOUNDARY PROTECTION | DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(23)	feedback to senders is disabled on protocol format validation failure.

SC-07(23)	BOUNDARY PROTECTION | DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(23)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-07(23)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].
	SC-07(23)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the disabling of feedback to senders on protocol format validation failure].

SC-07(24)	BOUNDARY PROTECTION | PERSONALLY IDENTIFIABLE INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(24)_ODP	***processing rules for systems that process personally identifiable information are defined;***
	SC-07(24)(a)	***<SC-07(24)_ODP processing rules>*** are applied to data elements of personally identifiable information on systems that process personally identifiable information;
	SC-07(24)(b)[01]	permitted processing is monitored at the external interfaces to the systems that process personally identifiable information;
	SC-07(24)(b)[02]	permitted processing is monitored at key internal boundaries within the systems that process personally identifiable information;
	SC-07(24)(c)	each processing exception is documented for systems that process personally identifiable information;
	SC-07(24)(d)[01]	exceptions for systems that process personally identifiable information are reviewed;
	SC-07(24)(d)[02]	exceptions for systems that process personally identifiable information that are no longer supported are removed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(24)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; personally identifiable information processing policies; list of key internal boundaries of the system; system design documentation; system configuration settings and associated documentation; enterprise security and privacy architecture documentation; system audit records; system security plan; privacy plan; personally identifiable information inventory documentation; data mapping documentation; other relevant documents or records].
	SC-07(24)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; system developer; organizational personnel with boundary protection responsibilities].

SC-07(24)	BOUNDARY PROTECTION | PERSONALLY IDENTIFIABLE INFORMATION	
	SC-07(24)-Test	[SELECT FROM: Mechanisms implementing boundary protection capabilities].

SC-07(25)	BOUNDARY PROTECTION | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(25)_ODP[01]	***the unclassified national security system prohibited from directly connecting to an external network is defined;***
	SC-07(25)_ODP[02]	***the boundary protection device required for a direct connection to an external network is defined;***
	SC-07(25)	the direct connection of ***<SC-07(25)_ODP[01] unclassified national security system>*** to an external network without the use of ***<SC-07(25)_ODP[02] boundary protection device>*** is prohibited.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(25)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-07(25)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].
	SC-07(25)-Test	[SELECT FROM: Mechanisms prohibiting the direct connection of unclassified national security systems to an external network].

SC-07(26)	BOUNDARY PROTECTION | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(26)_ODP	***the boundary protection device required for a direct connection to an external network is defined;***
	SC-07(26)	the direct connection of classified national security system to an external network without the use of a ***<SC-07(26)_ODP boundary protection device>*** is prohibited.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(26)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-07(26)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].

SC-07(26)	BOUNDARY PROTECTION | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS	
	SC-07(26)-Test	[SELECT FROM: Mechanisms prohibiting the direct connection of classified national security systems to an external network].

SC-07(27)	BOUNDARY PROTECTION | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(27)_ODP[01]	***the unclassified, non-national security system prohibited from directly connecting to an external network is defined;***
	SC-07(27)_ODP[02]	***the boundary protection device required for a direct connection of unclassified, non-national security system to an external network is defined;***
	SC-07(27)	the direct connection of ***<SC-07(27)_ODP[01] unclassified, non-national security system>*** to an external network without the use of a ***<SC-07(27)_ODP[02] boundary protection device>*** is prohibited.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(27)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-07(27)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].
	SC-07(27)-Test	[SELECT FROM: Mechanisms prohibiting the direct connection of unclassified, non-national security systems to an external network].

SC-07(28)	BOUNDARY PROTECTION | CONNECTIONS TO PUBLIC NETWORKS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(28)_ODP	***the system that is prohibited from directly connecting to a public network is defined;***
	SC-07(28)	the direct connection of the ***<SC-07(28)_ODP system>*** to a public network is prohibited.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(28)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].

SC-07(28)	BOUNDARY PROTECTION | CONNECTIONS TO PUBLIC NETWORKS	
	SC-07(28)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].
	SC-07(28)-Test	[SELECT FROM: Mechanisms prohibiting the direct connection of systems to an external network].

SC-07(29)	BOUNDARY PROTECTION | SEPARATE SUBNETS TO ISOLATE FUNCTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-07(29)_ODP[01]	***one of the following PARAMETER VALUES is selected: {physically; logically};***
	SC-07(29)_ODP[02]	***critical system components and functions to be isolated are defined;***
	SC-07(29)	subnetworks are separated ***<SC-07(29)_ODP[01] SELECTED PARAMETER VALUE>*** to isolate ***<SC-07(29)_ODP[02] critical system components and functions>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-07(29)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing boundary protection; system design documentation; system hardware and software; system architecture; system configuration settings and associated documentation; criticality analysis; system audit records; system security plan; other relevant documents or records].
	SC-07(29)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with boundary protection responsibilities].
	SC-07(29)-Test	[SELECT FROM: Mechanisms separating critical system components and functions].

SC-08	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-08_ODP	***one or more of the following PARAMETER VALUES is/are selected: {confidentiality; integrity};***
	SC-08	the ***<SC-08_ODP SELECTED PARAMETER VALUE(S)>*** of transmitted information is/are protected.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-08-Examine	[SELECT FROM: System and communications protection policy; procedures addressing transmission confidentiality and integrity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-08-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].

SC-08	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	
	SC-08-Test	[SELECT FROM: Mechanisms supporting and/or implementing transmission confidentiality and/or integrity].

SC-08(01)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-08(01)_ODP	***one or more of the following PARAMETER VALUES is/are selected: {prevent unauthorized disclosure of information; detect changes to information};***
	SC-08(01)	cryptographic mechanisms are implemented to ***<SC-08(01)_ODP SELECTED PARAMETER VALUE(S)>*** during transmission.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-08(01)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing transmission confidentiality and integrity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-08(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].
	SC-08(01)-Test	[SELECT FROM: Cryptographic mechanisms supporting and/or implementing transmission confidentiality and/or integrity; mechanisms supporting and/or implementing alternative physical safeguards; organizational processes for defining and implementing alternative physical safeguards].

SC-08(02)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PRE- AND POST-TRANSMISSION HANDLING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-08(02)_ODP	***one or more of the following PARAMETER VALUES is/are selected: {confidentiality; integrity};***
	SC-08(02)[01]	information ***<SC-08(02)_ODP SELECTED PARAMETER VALUE(S)>*** is/are maintained during preparation for transmission;
	SC-08(02)[02]	information ***<SC-08(02)_ODP SELECTED PARAMETER VALUE(S)>*** is/are maintained during reception.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-08(02)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing transmission confidentiality and integrity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-08(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].

SC-08(02)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PRE- AND POST-TRANSMISSION HANDLING	
	SC-08(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing transmission confidentiality and/or integrity].

SC-08(03)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-08(03)_ODP	***alternative physical controls to protect message externals are defined;***
	SC-08(03)	cryptographic mechanisms are implemented to protect message externals unless otherwise protected by ***<SC-08(03)_ODP alternative physical controls>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-08(03)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing transmission confidentiality and integrity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-08(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].
	SC-08(03)-Test	[SELECT FROM: Cryptographic mechanisms supporting and/or implementing transmission confidentiality and/or integrity for message externals; mechanisms supporting and/or implementing alternative physical safeguards; organizational processes for defining and implementing alternative physical safeguards].

SC-08(04)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL OR RANDOMIZE COMMUNICATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-08(04)_ODP	***alternative physical controls to protect against unauthorized disclosure of communication patterns are defined;***
	SC-08(04)	cryptographic mechanisms are implemented to conceal or randomize communication patterns unless otherwise protected by ***<SC-08(04)_ODP alternative physical controls>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-08(04)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing transmission confidentiality and integrity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-08(04)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].

SC-08(04)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL OR RANDOMIZE COMMUNICATIONS	
	SC-08(04)-Test	[SELECT FROM: Cryptographic mechanisms supporting and/or implementing concealment or randomization of communication patterns; mechanisms supporting and/or implementing alternative physical safeguards; organizational processes for defining and implementing alternative physical safeguards].

SC-08(05)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PROTECTED DISTRIBUTION SYSTEM	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-08(05)_ODP[01]	***the protected distribution system is defined;***
	SC-08(05)_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {prevent unauthorized disclosure of information; detect changes to information};***
	SC-08(05)	the ***<SC-08(05)_ODP[01] protected distribution system>*** is implemented to ***<SC-08(05)_ODP[02] SELECTED PARAMETER VALUE(S)>*** during transmission.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-08(05)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing transmission confidentiality and integrity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-08(05)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].
	SC-08(05)-Test	[SELECT FROM: Cryptographic mechanisms supporting and/or implementing concealment or randomization of communication patterns; mechanisms supporting and/or implementing protected distribution systems].

SC-09	TRANSMISSION CONFIDENTIALITY	
	[WITHDRAWN: Incorporated into SC-08.]	

SC-10	NETWORK DISCONNECT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-10_ODP	***a time period of inactivity after which the system terminates a network connection associated with a communication session is defined;***
	SC-10	the network connection associated with a communication session is terminated at the end of the session or after ***<SC-10_ODP time period>*** of inactivity.

SC-10	NETWORK DISCONNECT	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-10-Examine	[SELECT FROM: System and communications protection policy; procedures addressing network disconnect; system design documentation; security plan; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-10-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].
	SC-10-Test	[SELECT FROM: Mechanisms supporting and/or implementing a network disconnect capability].

SC-11	TRUSTED PATH	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-11_ODP[01]	***one of the following PARAMETER VALUES is selected: {physically; logically};***
	SC-11_ODP[02]	***security functions of the system are defined;***
	SC-11a.	a ***<SC-11_ODP[01] SELECTED PARAMETER VALUE>*** isolated trusted communication path is provided for communications between the user and the trusted components of the system;
	SC-11b.	users are permitted to invoke the trusted communication path for communications between the user and the ***<SC-11_ODP[02] security functions>*** of the system, including authentication and re-authentication, at a minimum.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-11-Examine	[SELECT FROM: System and communications protection policy; procedures addressing trusted communication paths; security plan; system design documentation; system configuration settings and associated documentation; assessment results from independent, testing organizations; system audit records; system security plan; other relevant documents or records].
	SC-11-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].
	SC-11-Test	[SELECT FROM: Mechanisms supporting and/or implementing trusted communication paths].

SC-11(01)	TRUSTED PATH | IRREFUTABLE COMMUNICATIONS PATH	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-11(01)_ODP	***security functions of the system are defined;***
	SC-11(01)(a)	a trusted communication path that is irrefutably distinguishable from other communication paths is provided;

SC-11(01)	TRUSTED PATH | IRREFUTABLE COMMUNICATIONS PATH	
	SC-11(01)(b)	the trusted communication path for communications between the ***<SC-11(01)_ODP security functions>*** of the system and the user is initiated.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-11(01)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing trusted communication paths; security plan; system design documentation; system configuration settings and associated documentation; assessment results from independent, testing organizations; system audit records; system security plan; other relevant documents or records].
	SC-11(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].
	SC-11(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing trusted communication paths].

SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-12_ODP	***requirements for key generation, distribution, storage, access, and destruction are defined;***
	SC-12[01]	cryptographic keys are established when cryptography is employed within the system in accordance with ***<SC-12_ODP requirements>***;
	SC-12[02]	cryptographic keys are managed when cryptography is employed within the system in accordance with ***<SC-12_ODP requirements>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-12-Examine	[SELECT FROM: System and communications protection policy; procedures addressing cryptographic key establishment and management; system design documentation; cryptographic mechanisms; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-12-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for cryptographic key establishment and/or management].
	SC-12-Test	[SELECT FROM: Mechanisms supporting and/or implementing cryptographic key establishment and management].

SC-12(01)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-12(01)	information availability is maintained in the event of the loss of cryptographic keys by users.

SC-12(01)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-12(01)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing cryptographic key establishment, management, and recovery; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-12(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for cryptographic key establishment or management].
	SC-12(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing cryptographic key establishment and management].

SC-12(02)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-12(02)_ODP	***one of the following PARAMETER VALUES is selected: {NIST FIPS-validated; NSA-approved};***
	SC-12(02)[01]	symmetric cryptographic keys are produced using ***<SC-12(02)_ODP SELECTED PARAMETER VALUE>*** key management technology and processes;
	SC-12(02)[02]	symmetric cryptographic keys are controlled using ***<SC-12(02)_ODP SELECTED PARAMETER VALUE>*** key management technology and processes;
	SC-12(02)[03]	symmetric cryptographic keys are distributed using ***<SC-12(02)_ODP SELECTED PARAMETER VALUE>*** key management technology and processes.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-12(02)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing cryptographic key establishment and management; system design documentation; system configuration settings and associated documentation; system audit records; list of FIPS-validated cryptographic products; list of NSA-approved cryptographic products; system security plan; other relevant documents or records].
	SC-12(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for cryptographic key establishment or management].
	SC-12(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing symmetric cryptographic key establishment and management].

SC-12(03)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-12(03)_ODP	***one of the following PARAMETER VALUES is selected: {NSA-approved key management technology and processes; prepositioned keying material; DoD-approved or DoD-issued Medium Assurance PKI certificates; DoD-approved or DoD-issued Medium Hardware Assurance PKI certificates and hardware security tokens that protect the user's private key; certificates issued in accordance with organization-defined requirements};***
	SC-12(03)[01]	asymmetric cryptographic keys are produced using ***<SC-12(03)_ODP SELECTED PARAMETER VALUE>***;
	SC-12(03)[02]	asymmetric cryptographic keys are controlled using ***<SC-12(03)_ODP SELECTED PARAMETER VALUE>***;
	SC-12(03)[03]	asymmetric cryptographic keys are distributed using ***<SC-12(03)_ODP SELECTED PARAMETER VALUE>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-12(03)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing cryptographic key establishment and management; system design documentation; system configuration settings and associated documentation; system audit records; list of NSA-approved cryptographic products; list of approved PKI Class 3 and Class 4 certificates; system security plan; other relevant documents or records].
	SC-12(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for cryptographic key establishment or management; organizational personnel with responsibilities for PKI certificates].
	SC-12(03)-Test	[SELECT FROM: Mechanisms supporting and/or implementing asymmetric cryptographic key establishment and management].

SC-12(04)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES
	[WITHDRAWN: Incorporated into SC-12(03).]

SC-12(05)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES / HARDWARE TOKENS
	[WITHDRAWN: Incorporated into SC-12(03).]

SC-12(06)	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PHYSICAL CONTROL OF KEYS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-12(06)	physical control of cryptographic keys is maintained when stored information is encrypted by external service providers.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-12(06)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing cryptographic key establishment, management, and recovery; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-12(06)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for cryptographic key establishment or management].
	SC-12(06)-Test	[SELECT FROM: Mechanisms supporting and/or implementing cryptographic key establishment and management].

SC-13	CRYPTOGRAPHIC PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-13_ODP[01]	***cryptographic uses are defined;***
	SC-13_ODP[02]	***types of cryptography for each specified cryptographic use are defined;***
	SC-13a.	***<SC-13_ODP[01] cryptographic uses>*** are identified;
	SC-13b.	***<SC-13_ODP[02] types of cryptography>*** for each specified cryptographic use (defined in SC-13_ODP[01]) are implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-13-Examine	[SELECT FROM: System and communications protection policy; procedures addressing cryptographic protection; system design documentation; system configuration settings and associated documentation; cryptographic module validation certificates; list of FIPS-validated cryptographic modules; system audit records; system security plan; other relevant documents or records].
	SC-13-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for cryptographic protection].
	SC-13-Test	[SELECT FROM: Mechanisms supporting and/or implementing cryptographic protection].

SC-13(01)	CRYPTOGRAPHIC PROTECTION | FIPS-VALIDATED CRYPTOGRAPHY
	[WITHDRAWN: Incorporated into SC-13.]

SC-13(02)	CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY
	[WITHDRAWN: Incorporated into SC-13.]

SC-13(03)	CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS
	[WITHDRAWN: Incorporated into SC-13.]

SC-13(04)	CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES
	[WITHDRAWN: Incorporated into SC-13.]

SC-14	PUBLIC ACCESS PROTECTIONS
	[WITHDRAWN: Incorporated into AC-02, AC-03, AC-05, AC-06, SI-03, SI-04, SI-05, SI-07, SI-10.]

SC-15	COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-15_ODP	***exceptions where remote activation is to be allowed are defined;***
	SC-15a.	remote activation of collaborative computing devices and applications is prohibited except ***<SC-15_ODP exceptions where remote activation is to be allowed>***;
	SC-15b.	an explicit indication of use is provided to users physically present at the devices.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-15-Examine	[SELECT FROM: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-15-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for managing collaborative computing devices].
	SC-15-Test	[SELECT FROM: Mechanisms supporting and/or implementing the management of remote activation of collaborative computing devices; mechanisms providing an indication of use of collaborative computing devices].

SC-15(01)	COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS | PHYSICAL OR LOGICAL DISCONNECT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-15(01)_ODP	***one or more of the following PARAMETER VALUES is/are selected: {physical; logical};***
	SC-15(01)	the ***<SC-15(01)_ODP SELECTED PARAMETER VALUE(S)>*** disconnect of collaborative computing devices is/are provided in a manner that supports ease of use.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-15(01)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-15(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for managing collaborative computing devices].
	SC-15(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the physical disconnect of collaborative computing devices].

SC-15(02)	COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS | BLOCKING INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC
	[WITHDRAWN: Incorporated into SC-07.]

SC-15(03)	COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS | DISABLING AND REMOVAL IN SECURE WORK AREAS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-15(03)_ODP[01]	***systems or system components from which collaborative computing devices are to be disabled or removed are defined;***
	SC-15(03)_ODP[02]	***secure work areas where collaborative computing devices are to be disabled or removed from systems or system components are defined;***
	SC-15(03)	collaborative computing devices and applications are disabled or removed from ***<SC-15(03)_ODP[01] systems or system components>*** in ***<SC-15(03)_ODP[02] secure work areas>***.

SC-15(03)	COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS | DISABLING AND REMOVAL IN SECURE WORK AREAS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-15(03)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; system design documentation; system configuration settings and associated documentation; system audit records; list of secure work areas; systems or system components in secured work areas where collaborative computing devices are to be disabled or removed; system security plan; other relevant documents or records].
	SC-15(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for managing collaborative computing devices].
	SC-15(03)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the capability to disable collaborative computing devices].

SC-15(04)	COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS | EXPLICITLY INDICATE CURRENT PARTICIPANTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-15(04)_ODP	***online meetings and teleconferences for which an explicit indication of current participants is to be provided are defined;***
	SC-15(04)	an explicit indication of current participants in ***<SC-15(04)_ODP online meetings and teleconferences>*** is provided.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-15(04)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; system design documentation; system configuration settings and associated documentation; system audit records; list of types of meetings and teleconferences requiring explicit indication of current participants; system security plan; other relevant documents or records].
	SC-15(04)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for managing collaborative computing devices].
	SC-15(04)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the capability to indicate participants on collaborative computing devices].

SC-16	TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-16_ODP[01]	***security attributes to be associated with information exchanged are defined;***
	SC-16_ODP[02]	***privacy attributes to be associated with information exchanged are defined;***

SC-16	TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES	
	SC-16[01]	***<SC-16_ODP[01] security attributes>*** are associated with information exchanged between systems;
	SC-16[02]	***<SC-16_ODP[01] security attributes>*** are associated with information exchanged between system components;
	SC-16[03]	***<SC-16_ODP[02] privacy attributes>*** are associated with information exchanged between systems;
	SC-16[04]	***<SC-16_ODP[02] privacy attributes>*** are associated with information exchanged between system components.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-16-Examine	[SELECT FROM: System and communications protection policy; procedures addressing the transmission of security and privacy attributes; access control policy and procedures; information flow control policy; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; other relevant documents or records].
	SC-16-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities].
	SC-16-Test	[SELECT FROM: Mechanisms supporting and/or implementing the transmission of security and privacy attributes between systems].

SC-16(01)	TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES | INTEGRITY VERIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-16(01)[01]	the integrity of transmitted security attributes is verified;
	SC-16(01)[02]	the integrity of transmitted privacy attributes is verified.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-16(01)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing the transmission of security and privacy attributes; access control policy and procedures; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; other relevant documents or records].
	SC-16(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities].
	SC-16(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing verification of the integrity of transmitted security and privacy attributes].

SC-16(02)	TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES | ANTI-SPOOFING MECHANISMS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-16(02)	anti-spoofing mechanisms are implemented to prevent adversaries from falsifying the security attributes indicating the successful application of the security process.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-16(02)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing the transmission of security and privacy attributes; access control policy and procedures; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-16(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	SC-16(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing anti-spoofing mechanisms].

SC-16(03)	TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES | CRYPTOGRAPHIC BINDING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-16(03)_ODP	***mechanisms or techniques to bind security and privacy attributes to transmitted information are defined;***
	SC-16(03)	***<SC-16(03)_ODP mechanisms or techniques>*** are implemented to bind security and privacy attributes to transmitted information.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-16(03)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing the transmission of security and privacy attributes; access control policy and procedures; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-16(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	SC-16(03)-Test	[SELECT FROM: Mechanisms supporting and/or implementing anti-spoofing mechanisms].

SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-17_ODP	***a certificate policy for issuing public key certificates is defined;***
	SC-17a.	public key certificates are issued under ***<SC-17_ODP certificate policy>*** , or public key certificates are obtained from an approved service provider;

SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	
	SC-17b.	only approved trust anchors are included in trust stores or certificate stores managed by the organization.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-17-Examine	[SELECT FROM: System and communications protection policy; procedures addressing public key infrastructure certificates; public key certificate policy or policies; public key issuing process; system security plan; other relevant documents or records].
	SC-17-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for issuing public key certificates; service providers].
	SC-17-Test	[SELECT FROM: Mechanisms supporting and/or implementing the management of public key infrastructure certificates].

SC-18	MOBILE CODE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-18a.[01]	acceptable mobile code is defined;
	SC-18a.[02]	unacceptable mobile code is defined;
	SC-18a.[03]	acceptable mobile code technologies are defined;
	SC-18a.[04]	unacceptable mobile code technologies are defined;
	SC-18b.[01]	the use of mobile code is authorized within the system;
	SC-18b.[02]	the use of mobile code is monitored within the system;
	SC-18b.[03]	the use of mobile code is controlled within the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-18-Examine	[SELECT FROM: System and communications protection policy; procedures addressing mobile code; mobile code implementation policy and procedures; list of acceptable mobile code and mobile code technologies; list of unacceptable mobile code and mobile technologies; authorization records; system monitoring records; system audit records; system security plan; other relevant documents or records].
	SC-18-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for managing mobile code].
	SC-18-Test	[SELECT FROM: Organizational process for authorizing, monitoring, and controlling mobile code; mechanisms supporting and/or implementing the management of mobile code; mechanisms supporting and/or implementing the monitoring of mobile code].

SC-18(01)	MOBILE CODE | IDENTIFY UNACCEPTABLE CODE AND TAKE CORRECTIVE ACTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-18(01)_ODP[01]	***unacceptable mobile code to be identified is defined;***
	SC-18(01)_ODP[02]	***corrective actions to be taken when unacceptable mobile code is identified are defined;***
	SC-18(01)[01]	***<SC-18(01)_ODP[01] unacceptable mobile code>*** is identified;
	SC-18(01)[02]	***<SC-18(01)_ODP[02] corrective actions>*** are taken if unacceptable mobile code is identified.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-18(01)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions; mobile code implementation policy and procedures; system design documentation; system configuration settings and associated documentation; list of unacceptable mobile code; list of corrective actions to be taken when unacceptable mobile code is identified; system monitoring records; system audit records; system security plan; other relevant documents or records].
	SC-18(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for managing mobile code].
	SC-18(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing mobile code detection, inspection, and corrective capabilities].

SC-18(02)	MOBILE CODE | ACQUISITION, DEVELOPMENT, AND USE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-18(02)_ODP	***mobile code requirements for the acquisition, development, and use of mobile code to be deployed in the system are defined;***
	SC-18(02)[01]	the acquisition of mobile code to be deployed in the system meets ***<SC-18(02)_ODP mobile code requirements>***;
	SC-18(02)[02]	the development of mobile code to be deployed in the system meets ***<SC-18(02)_ODP mobile code requirements>***;
	SC-18(02)[03]	the use of mobile code to be deployed in the system meets ***<SC-18(02)_ODP mobile code requirements>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-18(02)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing mobile code; mobile code requirements; mobile code usage restrictions; mobile code implementation policy and procedures; acquisition documentation; acquisition contracts for system, system component, or system service; system development life cycle documentation; system security plan; other relevant documents or records].

SC-18(02)	MOBILE CODE | ACQUISITION, DEVELOPMENT, AND USE	
	SC-18(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for managing mobile code; organizational personnel with acquisition and contracting responsibilities].
	SC-18(02)-Test	[SELECT FROM: Organizational processes for the acquisition, development, and use of mobile code].

SC-18(03)	MOBILE CODE | PREVENT DOWNLOADING AND EXECUTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-18(03)_ODP	***unacceptable mobile code to be prevented from downloading and executing is defined;***
	SC-18(03)[01]	the download of ***<SC-18(03)_ODP unacceptable mobile code>*** is prevented;
	SC-18(03)[02]	the execution of ***<SC-18(03)_ODP unacceptable mobile code>*** is prevented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-18(03)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions; mobile code implementation policy and procedures; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-18(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for managing mobile code].
	SC-18(03)-Test	[SELECT FROM: Mechanisms preventing the download and execution of unacceptable mobile code].

SC-18(04)	MOBILE CODE | PREVENT AUTOMATIC EXECUTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-18(04)_ODP[01]	***software applications in which the automatic execution of mobile code is to be prevented are defined;***
	SC-18(04)_ODP[02]	***actions to be enforced by the system prior to executing mobile code are defined;***
	SC-18(04)[01]	the automatic execution of mobile code in ***<SC-18(04)_ODP[01] software applications>*** is prevented;
	SC-18(04)[02]	***<SC-18(04)_ODP[02] actions>*** are enforced prior to executing mobile code.

SC-18(04)	MOBILE CODE | PREVENT AUTOMATIC EXECUTION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-18(04)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions; mobile code implementation policy and procedures; system design documentation; system configuration settings and associated documentation; list of software applications in which the automatic execution of mobile code must be prohibited; list of actions required before execution of mobile code; system security plan; other relevant documents or records].
	SC-18(04)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for managing mobile code].
	SC-18(04)-Test	[SELECT FROM: Mechanisms preventing the automatic execution of unacceptable mobile code; mechanisms enforcing actions to be taken prior to the execution of the mobile code].

SC-18(05)	MOBILE CODE | ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-18(05)	execution of permitted mobile code is allowed only in confined virtual machine environments.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-18(05)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing mobile code; mobile code usage allowances; mobile code usage restrictions; system design documentation; system configuration settings and associated documentation; list of confined virtual machine environments in which the execution of organizationally acceptable mobile code is allowed; system audit records; system security plan; other relevant documents or records].
	SC-18(05)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel with responsibilities for managing mobile code].
	SC-18(05)-Test	[SELECT FROM: Mechanisms allowing for the execution of permitted mobile code in confined virtual machine environments].

SC-19	VOICE OVER INTERNET PROTOCOL
	[WITHDRAWN. Technology-specific; addressed as any other technology or protocol.]

SC-20	SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-20a.[01]	additional data origin authentication is provided along with the authoritative name resolution data that the system returns in response to external name/address resolution queries;
	SC-20a.[02]	integrity verification artifacts are provided along with the authoritative name resolution data that the system returns in response to external name/address resolution queries;
	SC-20b.[01]	the means to indicate the security status of child zones (and if the child supports secure resolution services) is provided when operating as part of a distributed, hierarchical namespace;
	SC-20b.[02]	the means to enable verification of a chain of trust among parent and child domains when operating as part of a distributed, hierarchical namespace is provided.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-20-Examine	[SELECT FROM: System and communications protection policy; procedures addressing secure name/address resolution services (authoritative source); system design documentation; system configuration settings and associated documentation; system security plan; other relevant documents or records].
	SC-20-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for managing DNS].
	SC-20-Test	[SELECT FROM: Mechanisms supporting and/or implementing secure name/address resolution services].

SC-20(01)	SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | CHILD SUBSPACES
	[WITHDRAWN: Incorporated into SC-20.]

SC-20(02)	SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | DATA ORIGIN AND INTEGRITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-20(02)[01]	data origin artifacts are provided for internal name/address resolution queries;
	SC-20(02)[02]	integrity protection artifacts are provided for internal name/address resolution queries.

SC-20(02)	SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | DATA ORIGIN AND INTEGRITY	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-20(02)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing secure name/address resolution services (authoritative source); system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-20(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for managing DNS].
	SC-20(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing data origin and integrity protection for internal name/address resolution service queries].

SC-21	SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-21[01]	data origin authentication is requested for the name/address resolution responses that the system receives from authoritative sources;
	SC-21[02]	data origin authentication is performed on the name/address resolution responses that the system receives from authoritative sources;
	SC-21[03]	data integrity verification is requested for the name/address resolution responses that the system receives from authoritative sources;
	SC-21[04]	data integrity verification is performed on the name/address resolution responses that the system receives from authoritative sources.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-21-Examine	[SELECT FROM: System and communications protection policy; procedures addressing secure name/address resolution services (recursive or caching resolver); system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-21-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for managing DNS].
	SC-21-Test	[SELECT FROM: Mechanisms supporting and/or implementing data origin authentication and data integrity verification for name/address resolution services].

SC-21(01)	SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) | DATA ORIGIN AND INTEGRITY
	[WITHDRAWN: Incorporated into SC-21.]

SC-22	ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-22[01]	the systems that collectively provide name/address resolution services for an organization are fault-tolerant;
	SC-22[02]	the systems that collectively provide name/address resolution services for an organization implement internal role separation;
	SC-22[03]	the systems that collectively provide name/address resolution services for an organization implement external role separation.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-22-Examine	[SELECT FROM: System and communications protection policy; procedures addressing architecture and provisioning for name/address resolution services; access control policy and procedures; system design documentation; assessment results from independent testing organizations; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-22-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for managing DNS].
	SC-22-Test	[SELECT FROM: Mechanisms supporting and/or implementing name/address resolution services for fault tolerance and role separation].

SC-23	SESSION AUTHENTICITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-23	the authenticity of communication sessions is protected.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-23-Examine	[SELECT FROM: System and communications protection policy; procedures addressing session authenticity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-23-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	SC-23-Test	[SELECT FROM: Mechanisms supporting and/or implementing session authenticity].

SC-23(01)	SESSION AUTHENTICITY | INVALIDATE SESSION IDENTIFIERS AT LOGOUT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-23(01)	session identifiers are invalidated upon user logout or other session termination.

SC-23(01)	SESSION AUTHENTICITY | INVALIDATE SESSION IDENTIFIERS AT LOGOUT	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-23(01)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing session authenticity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-23(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	SC-23(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing session identifier invalidation upon session termination].

SC-23(02)	SESSION AUTHENTICITY | USER-INITIATED LOGOUTS AND MESSAGE DISPLAYS
	[WITHDRAWN: Incorporated into AC-12(01).]

SC-23(03)	SESSION AUTHENTICITY | UNIQUE SYSTEM-GENERATED SESSION IDENTIFIERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-23(03)_ODP	***randomness requirements for generating a unique session identifier for each session are defined;***
	SC-23(03)[01]	a unique session identifier is generated for each session with ***<SC-23(03)_ODP randomness requirements>***;
	SC-23(03)[02]	only system-generated session identifiers are recognized.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-23(03)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing session authenticity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-23(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	SC-23(03)-Test	[SELECT FROM: Mechanisms supporting, implementing, generating, and monitoring unique session identifiers; mechanisms supporting and/or implementing randomness requirements].

SC-23(04)	SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION
	[WITHDRAWN: Incorporated into SC-23(03).]

SC-23(05)	SESSION AUTHENTICITY | ALLOWED CERTIFICATE AUTHORITIES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-23(05)_ODP	***certificate authorities to be allowed for verification of the establishment of protected sessions are defined;***
	SC-23(05)	only the use of ***<SC-23(05)_ODP certificated authorities>*** for verification of the establishment of protected sessions is allowed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-23(05)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing session authenticity; system design documentation; system configuration settings and associated documentation; list of certificate authorities allowed for verification of the establishment of protected sessions; system audit records; system security plan; other relevant documents or records].
	SC-23(05)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	SC-23(05)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the management of certificate authorities].

SC-24	FAIL IN KNOWN STATE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-24_ODP[01]	***types of system failures for which the system components fail to a known state are defined;***
	SC-24_ODP[02]	***known system state to which system components fail in the event of a system failure is defined;***
	SC-24_ODP[03]	***system state information to be preserved in the event of a system failure is defined;***
	SC-24	***<SC-24_ODP[01] types of system failures on system components>*** fail to a ***<SC-24_ODP[02] known system state>*** while preserving ***<SC-24_ODP[03] system state information>*** in failure.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-24-Examine	[SELECT FROM: System and communications protection policy; procedures addressing system failure to known state; system design documentation; system configuration settings and associated documentation; list of failures requiring system to fail in a known state; state information to be preserved in system failure; system audit records; system security plan; other relevant documents or records].
	SC-24-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].
	SC-24-Test	[SELECT FROM: Mechanisms supporting and/or implementing the fail in known state capability; mechanisms preserving system state information in the event of a system failure].

SC-25	THIN NODES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-25_ODP	***system components to be employed with minimal functionality and information storage are defined;***
	SC-25[01]	minimal functionality for ***<SC-25_ODP system components>*** is employed;
	SC-25[02]	minimal information storage on ***<SC-25_ODP system components>*** is allocated.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-25-Examine	[SELECT FROM: System and communications protection policy; procedures addressing use of thin nodes; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-25-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	SC-25-Test	[SELECT FROM: Mechanisms supporting and/or implementing thin nodes].

SC-26	DECOYS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-26[01]	components within organizational systems specifically designed to be the target of malicious attacks are included to detect such attacks;
	SC-26[02]	components within organizational systems specifically designed to be the target of malicious attacks are included to deflect such attacks;
	SC-26[03]	components within organizational systems specifically designed to be the target of malicious attacks are included to analyze such attacks.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-26-Examine	[SELECT FROM: System and communications protection policy; procedures addressing the use of decoys; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-26-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].
	SC-26-Test	[SELECT FROM: Mechanisms supporting and/or implementing decoys].

SC-26(01)	DECOYS | DETECTION OF MALICIOUS CODE
	[WITHDRAWN: Incorporated into SC-35.]

SC-27	PLATFORM-INDEPENDENT APPLICATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-27_ODP	***platform-independent applications to be included within organizational systems are defined;***
	SC-27	***<SC-27_ODP platform-independent applications>*** are included within organizational systems.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-27-Examine	[SELECT FROM: System and communications protection policy; procedures addressing platform-independent applications; system design documentation; system configuration settings and associated documentation; list of platform-independent applications; system audit records; system security plan; other relevant documents or records].
	SC-27-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].
	SC-27-Test	[SELECT FROM: Mechanisms supporting and/or implementing platform-independent applications].

SC-28	PROTECTION OF INFORMATION AT REST	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-28_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {confidentiality; integrity};***
	SC-28_ODP[02]	***information at rest requiring protection is defined;***
	SC-28	the ***<SC-28_ODP[01] SELECTED PARAMETER VALUE(S)>*** of ***<SC-28_ODP[02] information at rest>*** is/are protected.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-28-Examine	[SELECT FROM: System and communications protection policy; procedures addressing the protection of information at rest; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; list of information at rest requiring confidentiality and integrity protections; system security plan; other relevant documents or records].
	SC-28-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].
	SC-28-Test	[SELECT FROM: Mechanisms supporting and/or implementing confidentiality and integrity protections for information at rest].

SC-28(01)	PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-28(01)_ODP[01]	***information requiring cryptographic protection is defined;***
	SC-28(01)_ODP[02]	***system components or media requiring cryptographic protection is/are defined;***
	SC-28(01)[01]	cryptographic mechanisms are implemented to prevent unauthorized disclosure of ***<SC-28(01)_ODP[01] information>*** at rest on ***<SC-28(01)_ODP[02] system components or media>***;
	SC-28(01)[02]	cryptographic mechanisms are implemented to prevent unauthorized modification of ***<SC-28(01)_ODP[01] information>*** at rest on ***<SC-28(01)_ODP[02] system components or media>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-28(01)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing the protection of information at rest; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; system audit records; system security plan; other relevant documents or records].
	SC-28(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].
	SC-28(01)-Test	[SELECT FROM: Cryptographic mechanisms implementing confidentiality and integrity protections for information at rest].

SC-28(02)	PROTECTION OF INFORMATION AT REST | OFFLINE STORAGE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-28(02)_ODP	***information to be removed from online storage and stored offline in a secure location is defined;***
	SC-28(02)[01]	***<SC-28(02)_ODP information>*** is removed from online storage;
	SC-28(02)[02]	***<SC-28(02)_ODP information>*** is stored offline in a secure location.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-28(02)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing the protection of information at rest; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; offline storage locations for information at rest; system audit records; system security plan; other relevant documents or records].
	SC-28(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	SC-28(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the removal of information from online storage; mechanisms supporting and/or implementing storage of information offline].

SC-28(03)	PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC KEYS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-28(03)_ODP[01]	***one of the following PARAMETER VALUES is selected: {<SC-28(03)_ODP[02] safeguards>; hardware-protected key store};***
	SC-28(03)_ODP[02]	***safeguards for protecting the storage of cryptographic keys are defined (if selected);***
	SC-28(03)	protected storage for cryptographic keys is provided using ***<SC-28(03)_ODP[01] SELECTED PARAMETER VALUE>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-28(03)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing the protection of information at rest; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; system audit records; system security plan; other relevant documents or records].
	SC-28(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities].
	SC-28(03)-Test	[SELECT FROM: Mechanisms supporting and/or implementing hardware-based key store protection].

SC-29	HETEROGENEITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-29_ODP	***system components requiring a diverse set of information technologies to be employed in the implementation of the system are defined;***
	SC-29	a diverse set of information technologies is employed for ***<SC-29_ODP system components>*** in the implementation of the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-29-Examine	[SELECT FROM: System and communications protection policy; system design documentation; system configuration settings and associated documentation; list of technologies deployed in the system; acquisition documentation; acquisition contracts for system components or services; system security plan; other relevant documents or records].
	SC-29-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with system acquisition, development, and implementation responsibilities].
	SC-29-Test	[SELECT FROM: Mechanisms supporting and/or implementing the employment of a diverse set of information technologies].

SC-29(01)	HETEROGENEITY | VIRTUALIZATION TECHNIQUES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-29(01)_ODP	***the frequency at which to change the diversity of operating systems and applications deployed using virtualization techniques is defined;***
	SC-29(01)	virtualization techniques are employed to support the deployment of a diverse range of operating systems and applications that are changed ***<SC-29(01)_ODP frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-29(01)-Examine	[SELECT FROM: System and communications protection policy; configuration management policy and procedures; system design documentation; system configuration settings and associated documentation; system architecture; list of operating systems and applications deployed using virtualization techniques; change control records; configuration management records; system audit records; system security plan; other relevant documents or records].
	SC-29(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with responsibilities for implementing approved virtualization techniques to the system].
	SC-29(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the employment of a diverse set of information technologies; mechanisms supporting and/or implementing virtualization techniques].

SC-30	CONCEALMENT AND MISDIRECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-30_ODP[01]	***concealment and misdirection techniques to be employed to confuse and mislead adversaries potentially targeting systems are defined;***
	SC-30_ODP[02]	***systems for which concealment and misdirection techniques are to be employed are defined;***
	SC-30_ODP[03]	***time periods to employ concealment and misdirection techniques for systems are defined;***
	SC-30	***<SC-30_ODP[01] concealment and misdirection techniques>*** are employed for ***<SC-30_ODP[02] systems>*** for ***<SC-30_ODP[03] time periods>*** to confuse and mislead adversaries.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-30-Examine	[SELECT FROM: System and communications protection policy; procedures addressing concealment and misdirection techniques for the system; system design documentation; system configuration settings and associated documentation; system architecture; list of concealment and misdirection techniques to be employed for organizational systems; system audit records; system security plan; other relevant documents or records].
	SC-30-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with the responsibility to implement concealment and misdirection techniques for systems].

SC-30	CONCEALMENT AND MISDIRECTION	
	SC-30-Test	[SELECT FROM: Mechanisms supporting and/or implementing concealment and misdirection techniques].

SC-30(01)	CONCEALMENT AND MISDIRECTION | VIRTUALIZATION TECHNIQUES
	[WITHDRAWN: Incorporated into SC-29(01).]

SC-30(02)	CONCEALMENT AND MISDIRECTION | RANDOMNESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-30(02)_ODP	***techniques employed to introduce randomness into organizational operations and assets are defined;***
	SC-30(02)	***<SC-30(02)_ODP techniques>*** are employed to introduce randomness into organizational operations and assets.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-30(02)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing concealment and misdirection techniques for the system; system design documentation; system configuration settings and associated documentation; system architecture; list of techniques to be employed to introduce randomness into organizational operations and assets; system audit records; system security plan; other relevant documents or records].
	SC-30(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with the responsibility to implement concealment and misdirection techniques for systems].
	SC-30(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing randomness as a concealment and misdirection technique].

SC-30(03)	CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING AND STORAGE LOCATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-30(03)_ODP[01]	***processing and/or storage locations to be changed are defined;***
	SC-30(03)_ODP[02]	***one of the following PARAMETER VALUES is selected: {<SC-30(03)_ODP[03] time frequency>; random time intervals};***
	SC-30(03)_ODP[03]	***time frequency at which to change the location of processing and/or storage is defined (if selected);***
	SC-30(03)	the location of ***<SC-30(03)_ODP[01] processing and/or storage>*** is changed ***<SC-30(03)_ODP[02] SELECTED PARAMETER VALUE>***.

SC-30(03)	CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING AND STORAGE LOCATIONS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-30(03)-Examine	[SELECT FROM: System and communications protection policy; configuration management policy and procedures; procedures addressing concealment and misdirection techniques for the system; list of processing/storage locations to be changed at organizational time intervals; change control records; configuration management records; system audit records; system security plan; other relevant documents or records].
	SC-30(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with the responsibility to change processing and/or storage locations].
	SC-30(03)-Test	[SELECT FROM: Mechanisms supporting and/or implementing changing processing and/or storage locations].

SC-30(04)	CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-30(04)_ODP	***system components for which realistic but misleading information about their security state or posture is employed are defined;***
	SC-30(04)	realistic but misleading information about the security state or posture of ***<SC-30(04)_ODP system components>*** is employed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-30(04)-Examine	[SELECT FROM: System and communications protection policy; configuration management policy and procedures; procedures addressing concealment and misdirection techniques for the system; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-30(04)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with the responsibility to define and employ realistic but misleading information about the security posture of system components].
	SC-30(04)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the employment of realistic but misleading information about the security posture of system components].

SC-30(05)	CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-30(05)_ODP[01]	***techniques to be employed to hide or conceal system components are defined;***
	SC-30(05)_ODP[02]	***system components to be hidden or concealed using techniques (defined in SC-30(05)_ODP[01]) are defined;***

SC-30(05)	CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS	
	SC-30(05)	***<SC-30(05)_ODP[01] techniques>*** are employed to hide or conceal ***<SC-30(05)_ODP[02] system components>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-30(05)-Examine	[SELECT FROM: System and communications protection policy; configuration management policy and procedures; procedures addressing concealment and misdirection techniques for the system; system design documentation; system configuration settings and associated documentation; list of techniques employed to hide or conceal system components; list of system components to be hidden or concealed; system security plan; other relevant documents or records].
	SC-30(05)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with the responsibility to conceal system components].
	SC-30(05)-Test	[SELECT FROM: Mechanisms supporting and/or implementing techniques for the concealment of system components].

SC-31	COVERT CHANNEL ANALYSIS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-31_ODP	***one or more of the following PARAMETER VALUES is/are selected: {storage; timing};***
	SC-31a.	a covert channel analysis is performed to identify those aspects of communications within the system that are potential avenues for covert ***<SC-31_ODP SELECTED PARAMETER VALUE(S)>*** channels;
	SC-31b.	the maximum bandwidth of those channels is estimated.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-31-Examine	[SELECT FROM: System and communications protection policy; procedures addressing covert channel analysis; system design documentation; system configuration settings and associated documentation; covert channel analysis documentation; system audit records; system security plan; other relevant documents or records].
	SC-31-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with covert channel analysis responsibilities; system developers/integrators].
	SC-31-Test	[SELECT FROM: Organizational process for conducting covert channel analysis; mechanisms supporting and/or implementing covert channel analysis; mechanisms supporting and/or implementing the capability to estimate the bandwidth of covert channels].

SC-31(01)	COVERT CHANNEL ANALYSIS | TEST COVERT CHANNELS FOR EXPLOITABILITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-31(01)	a subset of the identified covert channels is tested to determine the channels that are exploitable.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-31(01)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing covert channel analysis; system design documentation; system configuration settings and associated documentation; list of covert channels; covert channel analysis documentation; system audit records; system security plan; other relevant documents or records].
	SC-31(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with covert channel analysis responsibilities].
	SC-31(01)-Test	[SELECT FROM: Organizational process for testing covert channels; mechanisms supporting and/or implementing the testing of covert channel analysis].

SC-31(02)	COVERT CHANNEL ANALYSIS | MAXIMUM BANDWIDTH	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-31(02)_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {storage; timing};***
	SC-31(02)_ODP[02]	***values for the maximum bandwidth for identified covert channels are defined;***
	SC-31(02)	the maximum bandwidth for identified covert ***<SC-31(02)_ODP[01] SELECTED PARAMETER VALUE(S)>*** channels is reduced to ***<SC-31(02)_ODP[02] values>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-31(02)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing covert channel analysis; acquisition contracts for systems or services; acquisition documentation; system design documentation; system configuration settings and associated documentation; covert channel analysis documentation; system audit records; system security plan; other relevant documents or records].
	SC-31(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with covert channel analysis responsibilities; system developers/integrators].
	SC-31(02)-Test	[SELECT FROM: Organizational process for conducting covert channel analysis; mechanisms supporting and/or implementing covert channel analysis; mechanisms supporting and/or implementing the capability to reduce the bandwidth of covert channels].

SC-31(03)	COVERT CHANNEL ANALYSIS | MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-31(03)_ODP	***subset of identified covert channels whose bandwidth is to be measured in the operational environment of the system is defined;***
	SC-31(03)	the bandwidth of ***<SC-31(03)_ODP subset of identified covert channels>*** is measured in the operational environment of the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-31(03)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing covert channel analysis; system design documentation; system configuration settings and associated documentation; covert channel analysis documentation; system audit records; system security plan; other relevant documents or records].
	SC-31(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel with covert channel analysis responsibilities; system developers/integrators].
	SC-31(03)-Test	[SELECT FROM: Organizational process for conducting covert channel analysis; mechanisms supporting and/or implementing covert channel analysis; mechanisms supporting and/or implementing the capability to measure the bandwidth of covert channels].

SC-32	SYSTEM PARTITIONING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-32_ODP[01]	***system components to reside in separate physical or logical domains or environments based on circumstances for the physical or logical separation of components are defined;***
	SC-32_ODP[02]	***one of the following PARAMETER VALUES is selected: {physical; logical};***
	SC-32_ODP[03]	***circumstances for the physical or logical separation of components are defined;***
	SC-32	the system is partitioned into ***<SC-32_ODP[01] system components>*** residing in separate ***<SC-32_ODP[02] SELECTED PARAMETER VALUE>*** domains or environments based on ***<SC-32_ODP[03] circumstances for the physical or logical separation of components>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-32-Examine	[SELECT FROM: System and communications protection policy; procedures addressing system partitioning; system design documentation; system configuration settings and associated documentation; system architecture; list of system physical domains (or environments); system facility diagrams; system network diagrams; system security plan; other relevant documents or records].
	SC-32-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; system developers/integrators].

SC-32	SYSTEM PARTITIONING	
	SC-32-Test	[SELECT FROM: Mechanisms supporting and/or implementing the physical separation of system components].

SC-32(01)	SYSTEM PARTITIONING | SEPARATE PHYSICAL DOMAINS FOR PRIVILEGED FUNCTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-32(01)	privileged functions are partitioned into separate physical domains.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-32-Examine	[SELECT FROM: System and communications protection policy; procedures addressing system partitioning; system design documentation; system configuration settings and associated documentation; system architecture; list of system physical domains (or environments); system facility diagrams; system network diagrams; system security plan; other relevant documents or records].
	SC-32-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; system developers/integrators].
	SC-32-Test	[SELECT FROM: Mechanisms supporting and/or implementing the physical separation of system components].

SC-33	TRANSMISSION PREPARATION INTEGRITY
	[WITHDRAWN: Incorporated into SC-08.]

SC-34	NON-MODIFIABLE EXECUTABLE PROGRAMS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-34_ODP[01]	***system components for which the operating environment and applications are to be loaded and executed from hardware-enforced, read-only media are defined;***
	SC-34_ODP[02]	***applications to be loaded and executed from hardware-enforced, read-only media are defined;***
	SC-34a.	the operating environment for ***<SC-34_ODP[01] system components>*** is loaded and executed from hardware-enforced, read-only media;
	SC-34b.	***<SC-34_ODP[02] applications>*** for ***<SC-34_ODP[01] system components>*** are loaded and executed from hardware-enforced, read-only media.

SC-34	NON-MODIFIABLE EXECUTABLE PROGRAMS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-34-Examine	[SELECT FROM: System and communications protection policy; procedures addressing non-modifiable executable programs; system design documentation; system configuration settings and associated documentation; system architecture; list of operating system components to be loaded from hardware-enforced, read-only media; list of applications to be loaded from hardware-enforced, read-only media; media used to load and execute the system operating environment; media used to load and execute system applications; system audit records; system security plan; other relevant documents or records].
	SC-34-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel installing, configuring, and/or maintaining the system; system developers/integrators].
	SC-34-Test	[SELECT FROM: Mechanisms supporting and/or implementing, loading, and executing the operating environment from hardware-enforced, read-only media; mechanisms supporting and/or implementing, loading, and executing applications from hardware-enforced, read-only media].

SC-34(01)	NON-MODIFIABLE EXECUTABLE PROGRAMS | NO WRITABLE STORAGE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-34(01)_ODP	***system components to be employed with no writeable storage are defined;***
	SC-34(01)	***<SC-34(01)_ODP system components>*** are employed with no writeable storage that is persistent across component restart or power on/off.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-34(01)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing non-modifiable executable programs; system design documentation; system configuration settings and associated documentation; system architecture; list of system components to be employed without writeable storage capabilities; system audit records; system security plan; other relevant documents or records].
	SC-34(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; system developers/integrators].
	SC-34(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the employment of components with no writeable storage; mechanisms supporting and/or implementing persistent non-writeable storage across component restart and power on/off].

SC-34(02)	NON-MODIFIABLE EXECUTABLE PROGRAMS | INTEGRITY PROTECTION ON READ-ONLY MEDIA	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-34(02)[01]	the integrity of information is protected prior to storage on read-only media;
	SC-34(02)[02]	the media is controlled after such information has been recorded onto the media;
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-34(02)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing non-modifiable executable programs; system design documentation; system configuration settings and associated documentation; system architecture; system audit records; system security plan; other relevant documents or records].
	SC-34(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; system developers/integrators].
	SC-34(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the capability to protect information integrity on read-only media prior to storage and after information has been recorded onto the media].

SC-34(03)	NON-MODIFIABLE EXECUTABLE PROGRAMS | HARDWARE-BASED PROTECTION
	[WITHDRAWN: Moved to SC-51.]

SC-35	EXTERNAL MALICIOUS CODE IDENTIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-35	system components that proactively seek to identify network-based malicious code or malicious websites are included.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-35-Examine	[SELECT FROM: System and communications protection policy; procedures addressing external malicious code identification; system design documentation; system configuration settings and associated documentation; system components deployed to identify malicious websites and/or web-based malicious code; system audit records; system security plan; other relevant documents or records].
	SC-35-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; system developers/integrators].
	SC-35-Test	[SELECT FROM: Automated mechanisms supporting and/or implementing external malicious code identification].

SC-36	DISTRIBUTED PROCESSING AND STORAGE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-36_ODP[01]	***processing components to be distributed across multiple locations/domains are defined;***
	SC-36_ODP[02]	***one of the following PARAMETER VALUES is selected: {physical locations; logical domains};***
	SC-36_ODP[03]	***storage components to be distributed across multiple locations/domains are defined;***
	SC-36_ODP[04]	***one of the following PARAMETER VALUES is selected: {physical locations; logical domains};***
	SC-36[01]	***<SC-36_ODP[01] processing components>*** are distributed across ***<SC-36_ODP[02] SELECTED PARAMETER VALUE>***;
	SC-36[02]	***<SC-36_ODP[03] storage components>*** are distributed across ***<SC-36_ODP[04] SELECTED PARAMETER VALUE>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-36-Examine	[SELECT FROM: System and communications protection policy; contingency planning policy and procedures; contingency plan; system design documentation; system configuration settings and associated documentation; system architecture; list of system physical locations (or environments) with distributed processing and storage; system facility diagrams; processing site agreements; storage site agreements; system security plan; other relevant documents or records].
	SC-36-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel with contingency planning and plan implementation responsibilities; system developers/integrators].
	SC-36-Test	[SELECT FROM: Organizational processes for distributed processing and storage across multiple physical locations; mechanisms supporting and/or implementing the capability to distribute processing and storage across multiple physical locations].

SC-36(01)	DISTRIBUTED PROCESSING AND STORAGE | POLLING TECHNIQUES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-36(01)_ODP[01]	***distributed processing and storage components for which polling techniques are to be employed to identify potential faults, errors, or compromises are defined;***
	SC-36(01)_ODP[02]	***actions to be taken in response to identified faults, errors, or compromise are defined;***
	SC-36(01)(a)	polling techniques are employed to identify potential faults, errors, or compromises to ***<SC-36(01)_ODP[01] distributed processing and storage components>***;
	SC-36(01)(b)	***<SC-36(01)_ODP[02] actions>*** are taken in response to identified faults, errors, or compromise.

SC-36(01)	DISTRIBUTED PROCESSING AND STORAGE | POLLING TECHNIQUES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-36(01)-Examine	[SELECT FROM: System and communications protection policy; system design documentation; system configuration settings and associated documentation; system architecture; list of distributed processing and storage components subject to polling; system polling techniques and associated documentation or records; system audit records; system security plan; other relevant documents or records].
	SC-36(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; system developers/integrators].
	SC-36(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing polling techniques].

SC-36(02)	DISTRIBUTED PROCESSING AND STORAGE | SYNCHRONIZATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-36(02)_ODP	***duplicate systems or system components to be synchronized are defined;***
	SC-36(02)	***<SC-36(02)_ODP duplicate systems or system components>*** are synchronized.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-36(02)-Examine	[SELECT FROM: System and communications protection policy; system design documentation; system configuration settings and associated documentation; system architecture; list of distributed processing and storage components subject to polling; system polling techniques and associated documentation or records; system audit records; system security plan; other relevant documents or records].
	SC-36(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; system developers/integrators].
	SC-36(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing duplicate system or system component synchronization].

SC-37	OUT-OF-BAND CHANNELS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-37_ODP[01]	***out-of-band channels to be employed for the physical delivery or electronic transmission of information, system components, or devices to individuals or the system are defined;***
	SC-37_ODP[02]	***information, system components, or devices to employ out-of-band-channels for physical delivery or electronic transmission are defined;***
	SC-37_ODP[03]	***individuals or systems to which physical delivery or electronic transmission of information, system components, or devices is to be achieved via the employment of out-of-band channels are defined;***

SC-37	OUT-OF-BAND CHANNELS	
	SC-37	***<SC-37_ODP[01] out-of-band channels>*** are employed for the physical delivery or electronic transmission of ***<SC-37_ODP[02] information, system components, or devices>*** to ***<SC-37_ODP[03] individuals or systems>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-37-Examine	[SELECT FROM: System and communications protection policy; procedures addressing the use of out-of-band channels; access control policy and procedures; identification and authentication policy and procedures; system design documentation; system architecture; system configuration settings and associated documentation; list of out-of-band channels; types of information, system components, or devices requiring the use of out-of-band channels for physical delivery or electronic transmission to authorized individuals or systems; physical delivery records; electronic transmission records; system audit records; system security plan; other relevant documents or records].
	SC-37-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel authorizing, installing, configuring, operating, and/or using out-of-band channels; system developers/integrators].
	SC-37-Test	[SELECT FROM: Organizational processes for the use of out-of-band channels; mechanisms supporting and/or implementing the use of out-of-band channels].

SC-37(01)	OUT-OF-BAND CHANNELS | ENSURE DELIVERY AND TRANSMISSION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-37(01)_ODP[01]	***controls to be employed to ensure that only designated individuals or systems receive specific information, system components, or devices are defined;***
	SC-37(01)_ODP[02]	***individuals or systems designated to receive specific information, system components, or devices are defined;***
	SC-37(01)_ODP[03]	***information, system components, or devices that only individuals or systems are designated to receive are defined;***
	SC-37(01)	***<SC-37(01)_ODP[01] controls>*** are employed to ensure that only ***<SC-37(01)_ODP[02] individuals or systems>*** receive ***<SC-37(01)_ODP[03] information, system components, or devices>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-37(01)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing the use of out-of-band channels; access control policy and procedures; identification and authentication policy and procedures; system design documentation; system architecture; system configuration settings and associated documentation; list of security safeguards to be employed to ensure that designated individuals or systems receive organization-defined information, system components, or devices; list of security safeguards for delivering designated information, system components, or devices to designated individuals or systems; list of information, system components, or devices to be delivered to designated individuals or systems; system audit records; system security plan; other relevant documents or records].

SC-37(01)	OUT-OF-BAND CHANNELS | ENSURE DELIVERY AND TRANSMISSION	
	SC-37(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel authorizing, installing, configuring, operating, and/or using out-of-band channels; system developers/integrators].
	SC-37(01)-Test	[SELECT FROM: Organizational processes for the use of out-of-band channels; mechanisms supporting and/or implementing the use of out-of-band channels; mechanisms supporting/implementing safeguards to ensure the delivery of designated information, system components, or devices].

SC-38	OPERATIONS SECURITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-38_ODP	***operations security controls to be employed to protect key organizational information throughout the system development life cycle are defined;***
	SC-38	***<SC-38_ODP operations security controls>*** are employed to protect key organizational information throughout the system development life cycle.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-38-Examine	[SELECT FROM: System and communications protection policy; procedures addressing operations security; security plan; list of operations security safeguards; security control assessments; risk assessments; threat and vulnerability assessments; plans of action and milestones; system development life cycle documentation; system security plan; other relevant documents or records].
	SC-38-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; system developers/integrators].
	SC-38-Test	[SELECT FROM: Organizational processes for protecting organizational information throughout the system development life cycle; mechanisms supporting and/or implementing safeguards to protect organizational information throughout the system development life cycle].

SC-39	PROCESS ISOLATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-39	a separate execution domain is maintained for each executing system process.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-39-Examine	[SELECT FROM: System design documentation; system architecture; independent verification and validation documentation; testing and evaluation documentation; other relevant documents or records].
	SC-39-Interview	[SELECT FROM: System developers/integrators; system security architect].

SC-39	PROCESS ISOLATION	
	SC-39-Test	[SELECT FROM: Mechanisms supporting and/or implementing separate execution domains for each executing process].

SC-39(01)	PROCESS ISOLATION | HARDWARE SEPARATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-39(01)	hardware separation is implemented to facilitate process isolation.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-39(01)-Examine	[SELECT FROM: System and communications protection policy; system design documentation; system configuration settings and associated documentation; system architecture; system documentation for hardware separation mechanisms; system documentation from vendors, manufacturers, or developers; independent verification and validation documentation; system security plan; other relevant documents or records].
	SC-39(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; system developers/integrators].
	SC-39(01)-Test	[SELECT FROM: System capability implementing underlying hardware separation mechanisms for process separation].

SC-39(02)	PROCESS ISOLATION | SEPARATE EXECUTION DOMAIN PER THREAD	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-39(02)_ODP	***multi-thread processing for which a separate execution domain is to be maintained for each thread is defined;***
	SC-39(02)	a separate execution domain is maintained for each thread in ***<SC-39(02)_ODP multi-threaded processing>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-39(02)-Examine	[SELECT FROM: System and communications protection policy; system design documentation; system configuration settings and associated documentation; system architecture; list of system execution domains for each thread in multi-threaded processing; system documentation for multi-threaded processing; system documentation from vendors, manufacturers, or developers; independent verification and validation documentation; system security plan; other relevant documents or records].
	SC-39(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel installing, configuring, and/or maintaining the system; system developers/integrators].

SC-39(02)	PROCESS ISOLATION | SEPARATE EXECUTION DOMAIN PER THREAD	
	SC-39(02)-Test	[SELECT FROM: System capability implementing a separate execution domain for each thread in multi-threaded processing].

SC-40	WIRELESS LINK PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-40_ODP[01]	***external wireless links to be protected from particular types of signal parameter attacks are defined;***
	SC-40_ODP[02]	***types of signal parameter attacks or references to sources for such attacks from which to protect external wireless links are defined;***
	SC-40_ODP[03]	***internal wireless links to be protected from particular types of signal parameter attacks are defined;***
	SC-40_ODP[04]	***types of signal parameter attacks or references to sources for such attacks from which to protect internal wireless links are defined;***
	SC-40[01]	external ***<SC-40_ODP[01] wireless links>*** are protected from ***<SC-40_ODP[02] types of signal parameter attacks or references to sources for such attacks>***.
	SC-40[02]	internal ***<SC-40_ODP[03] wireless links>*** are protected from ***<SC-40_ODP[04] types of signal parameter attacks or references to sources for such attacks>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-40-Examine	[SELECT FROM: System and communications protection policy; access control policy and procedures; procedures addressing wireless link protection; system design documentation; wireless network diagrams; system configuration settings and associated documentation; system architecture; list of internal and external wireless links; list of signal parameter attacks or references to sources for attacks; system audit records; system security plan; other relevant documents or records].
	SC-40-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel authorizing, installing, configuring, and/or maintaining internal and external wireless links].
	SC-40-Test	[SELECT FROM: Mechanisms supporting and/or implementing the protection of wireless links].

SC-40(01)	WIRELESS LINK PROTECTION | ELECTROMAGNETIC INTERFERENCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-40(01)_ODP	***level of protection to be employed against the effects of intentional electromagnetic interference is defined;***
	SC-40(01)	cryptographic mechanisms that achieve ***<SC-40(01)_ODP level of protection>*** against the effects of intentional electromagnetic interference are implemented.

SC-40(01)	WIRELESS LINK PROTECTION | ELECTROMAGNETIC INTERFERENCE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-40(01)-Examine	[SELECT FROM: System and communications protection policy; access control policy and procedures; procedures addressing wireless link protection; system design documentation; wireless network diagrams; system configuration settings and associated documentation; system architecture; system communications hardware and software; security categorization results; system audit records; system security plan; other relevant documents or records].
	SC-40(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel authorizing, installing, configuring, and/or maintaining internal and external wireless links].
	SC-40(01)-Test	[SELECT FROM: Cryptographic mechanisms enforcing protections against effects of intentional electromagnetic interference].

SC-40(02)	WIRELESS LINK PROTECTION | REDUCE DETECTION POTENTIAL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-40(02)_ODP	***the level of reduction to be achieved to reduce the detection potential of wireless links is defined;***
	SC-40(02)	cryptographic mechanisms to reduce the detection potential of wireless links to ***<SC-40(02)_ODP level of reduction>*** are implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-40(02)-Examine	[SELECT FROM: System and communications protection policy; access control policy and procedures; procedures addressing wireless link protection; system design documentation; wireless network diagrams; system configuration settings and associated documentation; system architecture; system communications hardware and software; security categorization results; system audit records; system security plan; other relevant documents or records].
	SC-40(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel authorizing, installing, configuring, and/or maintaining internal and external wireless links].
	SC-40(02)-Test	[SELECT FROM: Cryptographic mechanisms enforcing protections to reduce the detection of wireless links].

SC-40(03)	WIRELESS LINK PROTECTION | IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-40(03)	cryptographic mechanisms are implemented to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-40(03)-Examine	[SELECT FROM: System and communications protection policy; access control policy and procedures; procedures addressing system design documentation; wireless network diagrams; system configuration settings and associated documentation; system architecture; system communications hardware and software; system audit records; system security plan; other relevant documents or records].
	SC-40(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel authorizing, installing, configuring, and/or maintaining internal and external wireless links].
	SC-40(03)-Test	[SELECT FROM: Cryptographic mechanisms enforcing wireless link protections against imitative or manipulative communications deception].

SC-40(04)	WIRELESS LINK PROTECTION | SIGNAL PARAMETER IDENTIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-40(04)_ODP	***wireless transmitters for which cryptographic mechanisms are to be implemented are defined;***
	SC-40(04)	cryptographic mechanisms are implemented to prevent the identification of ***<SC-40(04)_ODP wireless transmitters>*** by using the transmitter signal parameters.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-40(04)-Examine	[SELECT FROM: System and communications protection policy; access control policy and procedures; procedures addressing system design documentation; wireless network diagrams; system configuration settings and associated documentation; system architecture; system communications hardware and software; system audit records; system security plan; other relevant documents or records].
	SC-40(04)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel authorizing, installing, configuring, and/or maintaining internal and external wireless links].
	SC-40(04)-Test	[SELECT FROM: Cryptographic mechanisms preventing the identification of wireless transmitters].

SC-41	PORT AND I/O DEVICE ACCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-41_ODP[01]	***connection ports or input/output devices to be disabled or removed are defined;***
	SC-41_ODP[02]	***one of the following PARAMETER VALUES is selected: {physically; logically};***
	SC-41_ODP[03]	***systems or system components with connection ports or input/output devices to be disabled or removed are defined;***
	SC-41	***<SC-41_ODP[01] connection ports or input/output devices>*** are ***<SC-41_ODP[02] SELECTED PARAMETER VALUE>*** disabled or removed on ***<SC-41_ODP[03] systems or system components>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-41-Examine	[SELECT FROM: System and communications protection policy; access control policy and procedures; procedures addressing port and input/output device access; system design documentation; system configuration settings and associated documentation; system architecture; systems or system components; list of connection ports or input/output devices to be physically disabled or removed on systems or system components; system security plan; other relevant documents or records].
	SC-41-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system].
	SC-41-Test	[SELECT FROM: Mechanisms supporting and/or implementing the disabling of connection ports or input/output devices].

SC-42	SENSOR CAPABILITY AND DATA	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-42_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {the use of devices possessing <SC-42_ODP[02] environmental sensing capabilities> in <SC-42_ODP[03] facilities, areas, or systems>; the remote activation of environmental sensing capabilities on organizational systems or system components with the following exceptions: <SC-42_ODP[04] exceptions where remote activation of sensors is allowed>};***
	SC-42_ODP[02]	***environmental sensing capabilities in devices are defined (if selected);***
	SC-42_ODP[03]	***facilities, areas, or systems where the use of devices possessing environmental sensing capabilities is prohibited are defined (if selected);***
	SC-42_ODP[04]	***exceptions where remote activation of sensors is allowed are defined (if selected);***
	SC-42_ODP[05]	***group of users to whom an explicit indication of sensor use is to be provided is defined;***
	SC-42a.	***<SC-42_ODP[01] SELECTED PARAMETER VALUE(S)>*** is/are prohibited;
	SC-42b.	an explicit indication of sensor use is provided to ***<SC-42_ODP[05] group of users>***.

SC-42	SENSOR CAPABILITY AND DATA	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-42-Examine	[SELECT FROM: System and communications protection policy; procedures addressing sensor capabilities and data collection; access control policy and procedures; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; other relevant documents or records].
	SC-42-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; system developer; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for sensor capabilities].
	SC-42-Test	[SELECT FROM: Mechanisms implementing access controls for the remote activation of system sensor capabilities; mechanisms implementing the capability to indicate sensor use].

SC-42(01)	SENSOR CAPABILITY AND DATA | REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-42(01)_ODP	***sensors to be used to collect data or information are defined;***
	SC-42(01)	the system is configured so that data or information collected by the ***<SC-42(01)_ODP sensors>*** is only reported to authorized individuals or roles.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-42(01)-Examine	[SELECT FROM: System and communications protection policy; access control policy and procedures; procedures addressing sensor capability and data collection; personally identifiable information processing policy; system design documentation; system configuration settings and associated documentation; system architecture; system audit records; system security plan; privacy plan; other relevant documents or records].
	SC-42(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; system developer; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for the sensor capabilities].
	SC-42(01)-Test	[SELECT FROM: Mechanisms restricting the reporting of sensor information to those authorized; sensor data collection and reporting capabilities for the system].

SC-42(02)	SENSOR CAPABILITY AND DATA | AUTHORIZED USE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-42(02)_ODP	***measures to be employed so that data or information collected by sensors is only used for authorized purposes are defined;***
	SC-42(02)	***<SC-42(02)_ODP measures>*** are employed so that data or information collected by ***<SC-42(01)_ODP sensors>*** is only used for authorized purposes.

SC-42(02)	SENSOR CAPABILITY AND DATA | AUTHORIZED USE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-42(02)-Examine	[SELECT FROM: System and communications protection policy; access control policy and procedures; personally identifiable information processing policy; sensor capability and data collection; system design documentation; system configuration settings and associated documentation; system architecture; list of measures to be employed to that the ensure data or information collected by sensors is only used for authorized purposes; system audit records; system security plan; privacy plan; other relevant documents or records].
	SC-42(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for sensor capabilities].
	SC-42(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing measures to ensure that sensor information is only used for authorized purposes; sensor information collection capability for the system].

SC-42(03)	SENSOR CAPABILITY AND DATA | PROHIBIT USE OF DEVICES
	[WITHDRAWN: Incorporated into SC-42.]

SC-42(04)	SENSOR CAPABILITY AND DATA | NOTICE OF COLLECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-42(04)_ODP[01]	***measures to facilitate an individual's awareness that personally identifiable information is being collected are defined;***
	SC-42(04)_ODP[02]	***sensors that collect personally identifiable information are defined;***
	SC-42(04)	***<SC-42(04)_ODP[01] measures>*** are employed to facilitate an individual's awareness that personally identifiable information is being collected by ***<SC-42(04)_ODP[02] sensors>***
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-42(04)-Examine	[SELECT FROM: System and communications protection policy; access control policy and procedures; personally identifiable information processing policy; sensor capability and data collection policy and procedures; system design documentation; system configuration settings and associated documentation; privacy risk assessment documentation; privacy impact assessments; system architecture; list of measures to be employed to ensure that individuals are aware that personally identifiable information is being collected by sensors; examples of notifications provided to individuals that personally identifiable information is being collected by sensors; system audit records; system security plan; privacy plan; other relevant documents or records].
	SC-42(04)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for sensor capabilities].

SC-42(04)	SENSOR CAPABILITY AND DATA | NOTICE OF COLLECTION	
	SC-42(04)-Test	[SELECT FROM: Mechanisms supporting and/or implementing measures to facilitate an individual's awareness that personally identifiable information is being collected by sensors; sensor information collection capabilities for the system].

SC-42(05)	SENSOR CAPABILITY AND DATA | COLLECTION MINIMIZATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-42(05)_ODP	***the sensors that are configured to minimize the collection of unneeded information about individuals are defined;***
	SC-42(05)	the ***<SC-42(05)_ODP sensors>*** configured to minimize the collection of information about individuals that is not needed are employed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-42(05)-Examine	[SELECT FROM: System and communications protection policy; access control policy and procedures; personally identifiable information processing policy; sensor capability and data collection policy and procedures; system design documentation; system configuration settings and associated documentation; privacy risk assessment documentation; privacy impact assessments; system architecture; list of information being collected by sensors; list of sensor configurations that minimize the collection of personally identifiable information (e.g., obscure human features); system audit records; system security plan; privacy plan; other relevant documents or records].
	SC-42(05)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for sensor capabilities].
	SC-42(05)-Test	[SELECT FROM: Mechanisms supporting and/or implementing measures to facilitate the review of information that is being collected by sensors; sensor information collection capabilities for the system].

SC-43	USAGE RESTRICTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-43_ODP	***the components for which usage restrictions and implementation guidance are to be established are defined;***
	SC-43a.	usage restrictions and implementation guidelines are established for ***<SC-43_ODP components>***;
	SC-43b.[01]	the use of ***<SC-43_ODP components>*** is authorized within the system;
	SC-43b.[02]	the use of ***<SC-43_ODP components>*** is monitored within the system;
	SC-43b.[03]	the use of ***<SC-43_ODP components>*** is controlled within the system.

SC-43	USAGE RESTRICTIONS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-43-Examine	[SELECT FROM: System and communications protection policy; usage restrictions; procedures addressing usage restrictions; implementation policy and procedures; authorization records; system monitoring records; system audit records; system security plan; other relevant documents or records].
	SC-43-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system].
	SC-43-Test	[SELECT FROM: Organizational processes for authorizing, monitoring, and controlling the use of components with usage restrictions; mechanisms supporting and/or implementing, authorizing, monitoring, and controlling the use of components with usage restrictions].

SC-44	DETONATION CHAMBERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-44_ODP	***the system, system component, or location where a detonation chamber capability is to be employed is defined;***
	SC-44	a detonation chamber capability is employed within the ***<SC-44_ODP system, system component, or location>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-44-Examine	[SELECT FROM: System and communications protection policy; procedures addressing detonation chambers; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-44-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system].
	SC-44-Test	[SELECT FROM: Mechanisms supporting and/or implementing the detonation chamber capability].

SC-45	SYSTEM TIME SYNCHRONIZATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-45	system clocks are synchronized within and between systems and system components.

SC-45	SYSTEM TIME SYNCHRONIZATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-45-Examine	[SELECT FROM: System and communications protection policy; procedures addressing time synchronization; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-45-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system].
	SC-45-Test	[SELECT FROM: Mechanisms supporting and/or implementing system time synchronization].

SC-45(01)	SYSTEM TIME SYNCHRONIZATION | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-45(01)_ODP[01]	***the frequency at which to compare the internal system clocks with the authoritative time source is defined;***
	SC-45(01)_ODP[02]	***the authoritative time source to which internal system clocks are to be compared is defined;***
	SC-45(01)_ODP[03]	***the time period to compare the internal system clocks with the authoritative time source is defined;***
	SC-45(01)(a)	the internal system clocks are compared ***<SC-45(01)_ODP[01] frequency>*** with ***<SC-45(01)_ODP[02] authoritative time source>***;
	SC-45(01)(b)	the internal system clocks are synchronized with the authoritative time source when the time difference is greater than ***<SC-45(01)_ODP[03] time period>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-45(01)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing time synchronization; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-45(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system].
	SC-45(01)-Test	[SELECT FROM: Mechanisms supporting and/or implementing system time synchronization].

SC-45(02)	SYSTEM TIME SYNCHRONIZATION | SECONDARY AUTHORITATIVE TIME SOURCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-45(02)(a)	a secondary authoritative time source is identified that is in a different geographic region than the primary authoritative time source;
	SC-45(02)(b)	the internal system clocks are synchronized to the secondary authoritative time source if the primary authoritative time source is unavailable.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-45(02)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing time synchronization; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-45(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system].
	SC-45(02)-Test	[SELECT FROM: Mechanisms supporting and/or implementing system time synchronization with secondary authoritative time sources].

SC-46	CROSS DOMAIN POLICY ENFORCEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-46_ODP	***one of the following PARAMETER VALUES is selected: {physically; logically};***
	SC-46	a policy enforcement mechanism is ***<SC-46_ODP SELECTED PARAMETER VALUE>*** implemented between the physical and/or network interfaces for the connecting security domains.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-46-Examine	[SELECT FROM: System and communications protection policy; procedures addressing cross-domain policy enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-46-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system].
	SC-46-Test	[SELECT FROM: Mechanisms supporting and/or implementing cross-domain policy enforcement].

SC-47	ALTERNATE COMMUNICATIONS PATHS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-47_ODP	***alternate communication paths for system operations and operational command and control are defined;***
	SC-47	***<SC-47_ODP alternate communication paths>*** are established for system operations and operational command and control.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-47-Examine	[SELECT FROM: System and communications protection policy; procedures addressing communication paths; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-47-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers].
	SC-47-Test	[SELECT FROM: Mechanisms supporting and/or implementing alternate communication paths for system operations].

SC-48	SENSOR RELOCATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-48_ODP[01]	***sensors and monitoring capabilities to be relocated are defined;***
	SC-48_ODP[02]	***locations to where sensors and monitoring capabilities are to be relocated are defined;***
	SC-48_ODP[03]	***conditions or circumstances for relocating sensors and monitoring capabilities are defined;***
	SC-48	***<SC-48_ODP[01] sensors and monitoring capabilities>*** are relocated to ***<SC-48_ODP[02] locations>*** under ***<SC-48_ODP[03] conditions or circumstances>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-48-Examine	[SELECT FROM: System and communications protection policy; procedures addressing sensor and monitoring capability relocation; list of sensors/monitoring capabilities to be relocated; change control records; configuration management records; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-48-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system].
	SC-48-Test	[SELECT FROM: Mechanisms supporting and/or implementing sensor relocation].

SC-48(01)	SENSOR RELOCATION | DYNAMIC RELOCATION OF SENSORS OR MONITORING CAPABILITIES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-48(01)_ODP[01]	***sensors and monitoring capabilities to be dynamically relocated are defined;***
	SC-48(01)_ODP[02]	***locations to where sensors and monitoring capabilities are to be dynamically relocated are defined;***
	SC-48(01)_ODP[03]	***conditions or circumstances for dynamically relocating sensors and monitoring capabilities are defined;***
	SC-48(01)	***<SC-48(01)_ODP[01] sensors and monitoring capabilities>*** are dynamically relocated to ***<SC-48(01)_ODP[02] locations>*** under ***<SC-48(01)_ODP[03] conditions or circumstances>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-48(01)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing sensor and monitoring capability relocation; list of sensors/monitoring capabilities to be relocated; change control records; configuration management records; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-48(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system].
	SC-48(01)-Test	[SELECT FROM: SELECT FROM: Mechanisms supporting and/or implementing sensor relocation].

SC-49	HARDWARE-ENFORCED SEPARATION AND POLICY ENFORCEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-49_ODP	***security domains requiring hardware-enforced separation and policy enforcement mechanisms are defined;***
	SC-49	hardware-enforced separation and policy enforcement mechanisms are implemented between ***<SC-49_ODP security domains>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-49-Examine	[SELECT FROM: System and communications protection policy; procedures addressing cross-domain policy enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-49-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system].
	SC-49-Test	[SELECT FROM: Mechanisms supporting and/or implementing hardware-enforced security domain separation and policy enforcement].

SC-50	SOFTWARE-ENFORCED SEPARATION AND POLICY ENFORCEMENT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-50_ODP	***security domains requiring software-enforced separation and policy enforcement mechanisms are defined;***
	SC-50	software-enforced separation and policy enforcement mechanisms are implemented between ***<SC-50_ODP security domains>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-50-Examine	[SELECT FROM: System and communications protection policy; procedures addressing cross-domain policy enforcement; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-50-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system].
	SC-50-Test	[SELECT FROM: Mechanisms supporting and/or implementing software-enforced separation and policy enforcement].

SC-51	HARDWARE-BASED PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-51_ODP[01]	***system firmware components requiring hardware-based write-protect are defined;***
	SC-51_ODP[02]	***authorized individuals requiring procedures for disabling and re-enabling hardware write-protect are defined;***
	SC-51a.	hardware-based write-protect for ***<SC-51_ODP[01] system firmware components>*** is employed;
	SC-51b.[01]	specific procedures are implemented for ***<SC-51_ODP[02] authorized individuals>*** to manually disable hardware write-protect for firmware modifications;
	SC-51b.[02]	specific procedures are implemented for ***<SC-51_ODP[02] authorized individuals>*** to re-enable the write-protect prior to returning to operational mode.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-51-Examine	[SELECT FROM: System and communications protection policy; procedures addressing firmware modifications; system design documentation; system configuration settings and associated documentation; system architecture; system audit records; system security plan; other relevant documents or records].
	SC-51-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; system developers/integrators].
	SC-51-Test	[SELECT FROM: Organizational processes for modifying system firmware; mechanisms supporting and/or implementing hardware-based write-protection for system firmware].

4.19 SYSTEM AND INFORMATION INTEGRITY

SI-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-01_ODP[01]	***personnel or roles to whom the system and information integrity policy is to be disseminated is/are defined;***
	SI-01_ODP[02]	***personnel or roles to whom the system and information integrity procedures are to be disseminated is/are defined;***
	SI-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	SI-01_ODP[04]	***an official to manage the system and information integrity policy and procedures is defined;***
	SI-01_ODP[05]	***the frequency at which the current system and information integrity policy is reviewed and updated is defined;***
	SI-01_ODP[06]	***events that would require the current system and information integrity policy to be reviewed and updated are defined;***
	SI-01_ODP[07]	***the frequency at which the current system and information integrity procedures are reviewed and updated is defined;***
	SI-01_ODP[08]	***events that would require the system and information integrity procedures to be reviewed and updated are defined;***
	SI-01a.[01]	a system and information integrity policy is developed and documented;
	SI-01a.[02]	the system and information integrity policy is disseminated to ***<SI-01_ODP[01] personnel or roles>***;
	SI-01a.[03]	system and information integrity procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls are developed and documented;
	SI-01a.[04]	the system and information integrity procedures are disseminated to ***<SI-01_ODP[02] personnel or roles>***;
	SI-01a.01(a)[01]	the ***<SI-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and information integrity policy addresses purpose;
	SI-01a.01(a)[02]	the ***<SI-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and information integrity policy addresses scope;
	SI-01a.01(a)[03]	the ***<SI-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and information integrity policy addresses roles;
	SI-01a.01(a)[04]	the ***<SI-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and information integrity policy addresses responsibilities;
	SI-01a.01(a)[05]	the ***<SI-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and information integrity policy addresses management commitment;
	SI-01a.01(a)[06]	the ***<SI-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and information integrity policy addresses coordination among organizational entities;

SI-01	POLICY AND PROCEDURES	
	SI-01a.01(a)[07]	the ***<SI-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and information integrity policy addresses compliance;
	SI-01a.01(b)	the ***<SI-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** system and information integrity policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines;
	SI-01b.	the ***<SI-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the system and information integrity policy and procedures;
	SI-01c.01[01]	the current system and information integrity policy is reviewed and updated ***<SI-01_ODP[05] frequency>***;
	SI-01c.01[02]	the current system and information integrity policy is reviewed and updated following ***<SI-01_ODP[06] events>***;
	SI-01c.02[01]	the current system and information integrity procedures are reviewed and updated ***<SI-01_ODP[07] frequency>***;
	SI-01c.02[02]	the current system and information integrity procedures are reviewed and updated following ***<SI-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-01-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; system security plan; privacy plan; other relevant documents or records].
	SI-01-Interview	[SELECT FROM: Organizational personnel with system and information integrity responsibilities; organizational personnel with information security and privacy responsibilities].

SI-02	FLAW REMEDIATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-02_ODP	***time period within which to install security-relevant software updates after the release of the updates is defined;***
	SI-02a.[01]	system flaws are identified;
	SI-02a.[02]	system flaws are reported;
	SI-02a.[03]	system flaws are corrected;
	SI-02b.[01]	software updates related to flaw remediation are tested for effectiveness before installation;
	SI-02b.[02]	software updates related to flaw remediation are tested for potential side effects before installation;
	SI-02b.[03]	firmware updates related to flaw remediation are tested for effectiveness before installation;
	SI-02b.[04]	firmware updates related to flaw remediation are tested for potential side effects before installation;

SI-02	FLAW REMEDIATION	
	SI-02c.[01]	security-relevant software updates are installed within ***<SI-02_ODP time period>*** of the release of the updates;
	SI-02c.[02]	security-relevant firmware updates are installed within ***<SI-02_ODP time period>*** of the release of the updates;
	SI-02d.	flaw remediation is incorporated into the organizational configuration management process.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-02-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing flaw remediation; procedures addressing configuration management; list of flaws and vulnerabilities potentially affecting the system; list of recent security flaw remediation actions performed on the system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct system flaws); test results from the installation of software and firmware updates to correct system flaws; installation/change control records for security-relevant software and firmware updates; system security plan; privacy plan; other relevant documents or records].
	SI-02-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; organizational personnel responsible for installing, configuring, and/or maintaining the system; organizational personnel responsible for flaw remediation; organizational personnel with configuration management responsibilities].
	SI-02-Test	[SELECT FROM: Organizational processes for identifying, reporting, and correcting system flaws; organizational process for installing software and firmware updates; mechanisms supporting and/or implementing the reporting and correcting of system flaws; mechanisms supporting and/or implementing testing software and firmware updates].

SI-02(01)	FLAW REMEDIATION | CENTRAL MANAGEMENT	
	[WITHDRAWN: Incorporated into PL-09.]	

SI-02(02)	FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-02(02)_ODP[01]	***automated mechanisms to determine if applicable security-relevant software and firmware updates are installed on system components are defined;***
	SI-02(02)_ODP[02]	***the frequency at which to determine if applicable security-relevant software and firmware updates are installed on system components is defined;***
	SI-02(02)	system components have applicable security-relevant software and firmware updates installed ***<SI-02(02)_ODP[02] frequency>*** using ***<SI-02(02)_ODP[01] automated mechanisms>***.

SI-02(02)	FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-02(02)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing flaw remediation; automated mechanisms supporting centralized management of flaw remediation; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-02(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for flaw remediation].
	SI-02(02)-Test	[SELECT FROM: Automated mechanisms used to determine the state of system components with regard to flaw remediation].

SI-02(03)	FLAW REMEDIATION | TIME TO REMEDIATE FLAWS AND BENCHMARKS FOR CORRECTIVE ACTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-02(03)_ODP	***the benchmarks for taking corrective actions are defined;***
	SI-02(03)(a)	the time between flaw identification and flaw remediation is measured;
	SI-02(03)(b)	***<SI-02(03)_ODP benchmarks>*** for taking corrective actions have been established.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-02(03)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing flaw remediation; system design documentation; system configuration settings and associated documentation; list of benchmarks for taking corrective action on identified flaws; records that provide timestamps of flaw identification and subsequent flaw remediation activities; system security plan; other relevant documents or records].
	SI-02(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for flaw remediation].
	SI-02(03)-Test	[SELECT FROM: Organizational processes for identifying, reporting, and correcting system flaws; mechanisms used to measure the time between flaw identification and flaw remediation].

SI-02(04)	FLAW REMEDIATION | AUTOMATED PATCH MANAGEMENT TOOLS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-02(04)_ODP	***the system components requiring automated patch management tools to facilitate flaw remediation are defined;***

SI-02(04)	FLAW REMEDIATION | AUTOMATED PATCH MANAGEMENT TOOLS	
	SI-02(04)	automated patch management tools are employed to facilitate flaw remediation to ***<SI-02(04)_ODP components>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-02(04)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing flaw remediation; mechanisms supporting flaw remediation and automatic software/firmware updates; system design documentation; system configuration settings and associated documentation; list of system flaws; records of recent security-relevant software and firmware updates that are automatically installed to system components; system audit records; system security plan; other relevant documents or records].
	SI-02(04)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for flaw remediation].
	SI-02(04)-Test	[SELECT FROM: Automated patch management tools; mechanisms implementing automatic software/firmware updates; mechanisms facilitating flaw remediation to system components].

SI-02(05)	FLAW REMEDIATION | AUTOMATIC SOFTWARE AND FIRMWARE UPDATES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-02(05)_ODP[01]	***security-relevant software and firmware updates to be automatically installed to system components are defined;***
	SI-02(05)_ODP[02]	***system components requiring security-relevant software updates to be automatically installed are defined;***
	SI-02(05)	***<SI-02(05)_ODP[01] security-relevant software and firmware updates>*** are installed automatically to ***<SI-02(05)_ODP[02] system components>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-02(05)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing flaw remediation; mechanisms supporting flaw remediation and automatic software/firmware updates; system design documentation; system configuration settings and associated documentation; records of recent security-relevant software and firmware updates automatically installed to system components; system audit records; system security plan; other relevant documents or records].
	SI-02(05)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for flaw remediation].
	SI-02(05)-Test	[SELECT FROM: Mechanisms implementing automatic software/firmware updates].

SI-02(06)	FLAW REMEDIATION | REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE AND FIRMWARE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-02(06)_ODP	***software and firmware components to be removed after updated versions have been installed are defined;***
	SI-02(06)	previous versions of ***<SI-02(06)_ODP software and firmware components>*** are removed after updated versions have been installed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-02(06)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing flaw remediation; mechanisms supporting flaw remediation; system design documentation; system configuration settings and associated documentation; records of software and firmware component removals after updated versions are installed; system audit records; system security plan; other relevant documents or records].
	SI-02(06)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for flaw remediation].
	SI-02(06)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the removal of previous versions of software/firmware].

SI-03	MALICIOUS CODE PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-03_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {signature-based; non-signature-based};***
	SI-03_ODP[02]	***the frequency at which malicious code protection mechanisms perform scans is defined;***
	SI-03_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {endpoint; network entry and exit points};***
	SI-03_ODP[04]	***one or more of the following PARAMETER VALUES is/are selected: {block malicious code; quarantine malicious code; take <SI-03_ODP[05] action>};***
	SI-03_ODP[05]	***action to be taken in response to malicious code detection are defined (if selected);***
	SI-03_ODP[06]	***personnel or roles to be alerted when malicious code is detected is/are defined;***
	SI-03a.[01]	***<SI-03_ODP[01] SELECTED PARAMETER VALUE(S)>*** malicious code protection mechanisms are implemented at system entry and exit points to detect malicious code;
	SI-03a.[02]	***<SI-03_ODP[01] SELECTED PARAMETER VALUE(S)>*** malicious code protection mechanisms are implemented at system entry and exit points to eradicate malicious code;

SI-03	MALICIOUS CODE PROTECTION	
	SI-03b.	malicious code protection mechanisms are updated automatically as new releases are available in accordance with organizational configuration management policy and procedures;
	SI-03c.01[01]	malicious code protection mechanisms are configured to perform periodic scans of the system ***<SI-03_ODP[02] frequency>***;
	SI-03c.01[02]	malicious code protection mechanisms are configured to perform real-time scans of files from external sources at ***<SI-03_ODP[03] SELECTED PARAMETER VALUE(S)>*** as the files are downloaded, opened, or executed in accordance with organizational policy;
	SI-03c.02[01]	malicious code protection mechanisms are configured to ***<SI-03_ODP[04] SELECTED PARAMETER VALUE(S)>*** in response to malicious code detection;
	SI-03c.02[02]	malicious code protection mechanisms are configured to send alerts to ***<SI-03_ODP[06] personnel or roles>*** in response to malicious code detection;
	SI-03d.	the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system are addressed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-03-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; configuration management policy and procedures; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; system design documentation; system configuration settings and associated documentation; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; system audit records; system security plan; other relevant documents or records].
	SI-03-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for malicious code protection; organizational personnel with configuration management responsibilities].
	SI-03-Test	[SELECT FROM: Organizational processes for employing, updating, and configuring malicious code protection mechanisms; organizational processes for addressing false positives and resulting potential impacts; mechanisms supporting and/or implementing, employing, updating, and configuring malicious code protection mechanisms; mechanisms supporting and/or implementing malicious code scanning and subsequent actions].

SI-03(01)	MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT
	[WITHDRAWN: Incorporated into PL-09.]

SI-03(02)	MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES
	[WITHDRAWN: Incorporated into SI-03.]

SI-03(03)	MALICIOUS CODE PROTECTION | NON-PRIVILEGED USERS
	[WITHDRAWN: Incorporated into AC-06(10).]

SI-03(04)	MALICIOUS CODE PROTECTION | UPDATES ONLY BY PRIVILEGED USERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-03(04)	malicious code protection mechanisms are updated only when directed by a privileged user.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-03(04)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing malicious code protection; list of privileged users on system; system design documentation; malicious code protection mechanisms; records of malicious code protection updates; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-03(04)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for malicious code protection].
	SI-03(04)-Test	[SELECT FROM: Mechanisms supporting and/or implementing malicious code protection capabilities].

SI-03(05)	MALICIOUS CODE PROTECTION | PORTABLE STORAGE DEVICES
	[WITHDRAWN: Incorporated into MP-07.]

SI-03(06)	MALICIOUS CODE PROTECTION | TESTING AND VERIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-03(06)_ODP	***the frequency at which to test malicious code protection mechanisms is defined;***
	SI-03(06)(a)	malicious code protection mechanisms are tested ***<SI-03(06)_ODP frequency>*** by introducing known benign code into the system;
	SI-03(06)(b)[01]	the detection of (benign test) code occurs;
	SI-03(06)(b)[02]	the associated incident reporting occurs.

SI-03(06)	MALICIOUS CODE PROTECTION | TESTING AND VERIFICATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-03(06)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing malicious code protection; system design documentation; system configuration settings and associated documentation; test cases; records providing evidence of test cases executed on malicious code protection mechanisms; system audit records; system security plan; other relevant documents or records].
	SI-03(06)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for malicious code protection].
	SI-03(06)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the testing and verification of malicious code protection capabilities].

SI-03(07)	MALICIOUS CODE PROTECTION | NONSIGNATURE-BASED DETECTION
	[WITHDRAWN: Incorporated into SI-03.]

SI-03(08)	MALICIOUS CODE PROTECTION | DETECT UNAUTHORIZED COMMANDS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-03(08)_ODP[01]	***system hardware components for which unauthorized operating system commands are to be detected through the kernel application programming interface are defined;***
	SI-03(08)_ODP[02]	***unauthorized operating system commands to be detected are defined;***
	SI-03(08)_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {issue a warning; audit the command execution; prevent the execution of the command};***
	SI-03(08)(a)	***<SI-03(08)_ODP[01] unauthorized operating system commands>*** are detected through the kernel application programming interface on ***<SI-03(08)_ODP[02] system hardware components>***;
	SI-03(08)(b)	***<SI-03(08)_ODP[03] SELECTED PARAMETER VALUE(S)>*** is/are performed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-03(08)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing malicious code protection; system design documentation; malicious code protection mechanisms; warning messages sent upon the detection of unauthorized operating system command execution; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-03(08)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for malicious code protection].

SI-03(08)	MALICIOUS CODE PROTECTION | DETECT UNAUTHORIZED COMMANDS	
	SI-03(08)-Test	[SELECT FROM: Mechanisms supporting and/or implementing malicious code protection capabilities; mechanisms supporting and/or implementing the detection of unauthorized operating system commands through the kernel application programming interface].

SI-03(09)	MALICIOUS CODE PROTECTION | AUTHENTICATE REMOTE COMMANDS
	[WITHDRAWN: Moved to AC-17(10).]

SI-03(10)	MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-03(10)_ODP	***tools and techniques to be employed to analyze the characteristics and behavior of malicious code are defined;***
	SI-03(10)(a)	***<SI-03(10)_ODP tools and techniques>*** are employed to analyze the characteristics and behavior of malicious code;
	SI-03(10)(b)[01]	the results from malicious code analysis are incorporated into organizational incident response processes;
	SI-03(10)(b)[02]	the results from malicious code analysis are incorporated into organizational flaw remediation processes.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-03(10)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing malicious code protection; procedures addressing incident response; procedures addressing flaw remediation; system design documentation; malicious code protection mechanisms, tools, and techniques; system configuration settings and associated documentation; results from malicious code analyses; records of flaw remediation events resulting from malicious code analyses; system audit records; system security plan; other relevant documents or records].
	SI-03(10)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for malicious code protection; organizational personnel responsible for flaw remediation; organizational personnel responsible for incident response/ management].
	SI-03(10)-Test	[SELECT FROM: Organizational process for incident response; organizational process for flaw remediation; mechanisms supporting and/or implementing malicious code protection capabilities; tools and techniques for the analysis of malicious code characteristics and behavior].

SI-04	SYSTEM MONITORING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04_ODP[01]	***monitoring objectives to detect attacks and indicators of potential attacks on the system are defined;***
	SI-04_ODP[02]	***techniques and methods used to identify unauthorized use of the system are defined;***
	SI-04_ODP[03]	***system monitoring information to be provided to personnel or roles is defined;***
	SI-04_ODP[04]	***personnel or roles to whom system monitoring information is to be provided is/are defined;***
	SI-04_ODP[05]	***one or more of the following PARAMETER VALUES is/are selected: {as needed; <SI-04_ODP[06] frequency>};***
	SI-04_ODP[06]	***a frequency for providing system monitoring to personnel or roles is defined (if selected);***
	SI-04a.01	the system is monitored to detect attacks and indicators of potential attacks in accordance with ***<SI-04_ODP[01] monitoring objectives>***;
	SI-04a.02[01]	the system is monitored to detect unauthorized local connections;
	SI-04a.02[02]	the system is monitored to detect unauthorized network connections;
	SI-04a.02[03]	the system is monitored to detect unauthorized remote connections;
	SI-04b.	unauthorized use of the system is identified through ***<SI-04_ODP[02] techniques and methods>***;
	SI-04c.01	internal monitoring capabilities are invoked or monitoring devices are deployed strategically within the system to collect organization-determined essential information;
	SI-04c.02	internal monitoring capabilities are invoked or monitoring devices are deployed at ad hoc locations within the system to track specific types of transactions of interest to the organization;
	SI-04d.[01]	detected events are analyzed;
	SI-04d.[02]	detected anomalies are analyzed;
	SI-04e.	the level of system monitoring activity is adjusted when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;
	SI-04f.	a legal opinion regarding system monitoring activities is obtained;
	SI-04g.	***<SI-04_ODP[03] system monitoring information>*** is provided to ***<SI-04_ODP[04] personnel or roles> <SI-04_ODP[05] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; continuous monitoring strategy; facility diagram/layout; system design documentation; system monitoring tools and techniques documentation; locations within the system where monitoring devices are deployed; system configuration settings and associated documentation; system security plan; other relevant documents or records].

SI-04	SYSTEM MONITORING	
	SI-04-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system].
	SI-04-Test	[SELECT FROM: Organizational processes for system monitoring; mechanisms supporting and/or implementing system monitoring capabilities].

SI-04(01)	SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(01)[01]	individual intrusion detection tools are connected to a system-wide intrusion detection system;
	SI-04(01)[02]	individual intrusion detection tools are configured into a system-wide intrusion detection system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(01)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-04(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system].
	SI-04(01)-Test	[SELECT FROM: Organizational processes for intrusion detection and system monitoring; mechanisms supporting and/or implementing intrusion detection capabilities].

SI-04(02)	SYSTEM MONITORING | AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(02)	automated tools and mechanisms are employed to support a near real-time analysis of events.

SI-04(02)	SYSTEM MONITORING | AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(02)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; privacy program plan; privacy impact assessment; privacy risk management documentation; other relevant documents or records].
	SI-04(02)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for incident response/management].
	SI-04(02)-Test	[SELECT FROM: Organizational processes for the near real-time analysis of events; organizational processes for system monitoring; mechanisms supporting and/or implementing system monitoring; mechanisms/tools supporting and/or implementing an analysis of events].

SI-04(03)	SYSTEM MONITORING | AUTOMATED TOOL AND MECHANISM INTEGRATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(03)[01]	automated tools and mechanisms are employed to integrate intrusion detection tools and mechanisms into access control mechanisms;
	SI-04(03)[02]	automated tools and mechanisms are employed to integrate intrusion detection tools and mechanisms into flow control mechanisms.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(03)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; access control policy and procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-04(03)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system].
	SI-04(03)-Test	[SELECT FROM: Organizational processes for intrusion detection and system monitoring; mechanisms supporting and/or implementing the intrusion detection and system monitoring capability; mechanisms and tools supporting and/or implementing the access and flow control capabilities; mechanisms and tools supporting and/or implementing the integration of intrusion detection tools into the access and flow control mechanisms].

SI-04(04)	SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(04)_ODP[01]	***the frequency at which to monitor inbound communications traffic for unusual or unauthorized activities or conditions is defined;***
	SI-04(04)_ODP[02]	***unusual or unauthorized activities or conditions that are to be monitored in inbound communications traffic are defined;***
	SI-04(04)_ODP[03]	***the frequency at which to monitor outbound communications traffic for unusual or unauthorized activities or conditions is defined;***
	SI-04(04)_ODP[04]	***unusual or unauthorized activities or conditions that are to be monitored in outbound communications traffic are defined;***
	SI-04(04)(a)[01]	criteria for unusual or unauthorized activities or conditions for inbound communications traffic are defined;
	SI-04(04)(a)[02]	criteria for unusual or unauthorized activities or conditions for outbound communications traffic are defined;
	SI-04(04)(b)[01]	inbound communications traffic is monitored ***<SI-04(04)_ODP[01] frequency>*** for ***<SI-04(04)_ODP[02] unusual or unauthorized activities or conditions>***;
	SI-04(04)(b)[02]	outbound communications traffic is monitored ***<SI-04(04)_ODP[03] frequency>*** for ***<SI-04(04)_ODP[04] unusual or unauthorized activities or conditions>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(04)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system protocols; system audit records; system security plan; other relevant documents or records].
	SI-04(04)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system].
	SI-04(04)-Test	[SELECT FROM: Organizational processes for intrusion detection and system monitoring; mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; mechanisms supporting and/or implementing the monitoring of inbound and outbound communications traffic].

SI-04(05)	SYSTEM MONITORING | SYSTEM-GENERATED ALERTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(05)_ODP[01]	***personnel or roles to be alerted when indications of compromise or potential compromise occur is/are defined;***
	SI-04(05)_ODP[02]	***compromise indicators are defined;***

SI-04(05)	SYSTEM MONITORING | SYSTEM-GENERATED ALERTS	
	SI-04(05)	***<SI-04(05)_ODP[01] personnel or roles>*** are alerted when system-generated ***<SI-04(05)_ODP[02] compromise indicators>*** occur.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(05)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system monitoring tools and techniques documentation; system configuration settings and associated documentation; list of personnel selected to receive alerts; documentation of alerts generated based on compromise indicators; system audit records; system security plan; privacy plan; other relevant documents or records].
	SI-04(05)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; system developers; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel on the system alert notification list; organizational personnel responsible for the intrusion detection system].
	SI-04(05)-Test	[SELECT FROM: Organizational processes for intrusion detection and system monitoring; mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; mechanisms supporting and/or implementing alerts for compromise indicators].

SI-04(06)	SYSTEM MONITORING | RESTRICT NON-PRIVILEGED USERS
	[WITHDRAWN: Incorporated into AC-06(10).]

SI-04(07)	SYSTEM MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(07)_ODP[01]	***incident response personnel (identified by name and/or by role) to be notified of detected suspicious events is/are defined;***
	SI-04(07)_ODP[02]	***least-disruptive actions to terminate suspicious events are defined;***
	SI-04(07)(a)	***<SI-04(07)_ODP[01] incident response personnel>*** are notified of detected suspicious events;
	SI-04(07)(b)	***<SI-04(07)_ODP[02] least-disruptive actions>*** are taken upon the detection of suspicious events.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(07)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; alerts and notifications generated based on detected suspicious events; records of actions taken to terminate suspicious events; system audit records; system security plan; other relevant documents or records].

SI-04(07)	SYSTEM MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS	
	SI-04(07)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developers; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system].
	SI-04(07)-Test	[SELECT FROM: Organizational processes for intrusion detection and system monitoring; mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; mechanisms supporting and/or implementing notifications to incident response personnel; mechanisms supporting and/or implementing actions to terminate suspicious events].

SI-04(08)	SYSTEM MONITORING | PROTECTION OF MONITORING INFORMATION	
	[WITHDRAWN: Incorporated into SI-04.]	

SI-04(09)	SYSTEM MONITORING | TESTING OF MONITORING TOOLS AND MECHANISMS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(09)_ODP	***a frequency at which to test intrusion-monitoring tools and mechanisms is defined;***
	SI-04(09)	intrusion-monitoring tools and mechanisms are tested ***<SI-04(09)_ODP frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(09)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing the testing of system monitoring tools and techniques; documentation providing evidence of testing intrusion-monitoring tools; system security plan; other relevant documents or records].
	SI-04(09)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system].
	SI-04(09)-Test	[SELECT FROM: Organizational processes for intrusion detection and system monitoring; mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; mechanisms supporting and/or implementing the testing of intrusion-monitoring tools].

SI-04(10)	SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(10)_ODP[01]	***encrypted communications traffic to be made visible to system monitoring tools and mechanisms is defined;***

SI-04(10)	SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS	
	SI-04(10)_ODP[02]	***system monitoring tools and mechanisms to be provided access to encrypted communications traffic are defined;***
	SI-04(10)	provisions are made so that ***<SI-04(10)_ODP[01] encrypted communications traffic>*** is visible to ***<SI-04(10)_ODP[02] system monitoring tools and mechanisms>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(10)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system protocols; system security plan; other relevant documents or records].
	SI-04(10)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system].
	SI-04(10)-Test	[SELECT FROM: Organizational processes for intrusion detection and system monitoring; mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; mechanisms supporting and/or implementing the visibility of encrypted communications traffic to monitoring tools].

SI-04(11)	SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(11)_ODP	***interior points within the system where communications traffic is to be analyzed are defined;***
	SI-04(11)[01]	outbound communications traffic at the external interfaces to the system is analyzed to discover anomalies;
	SI-04(11)[02]	outbound communications traffic at ***<SI-04(11)_ODP interior points>*** is analyzed to discover anomalies.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(11)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; network diagram; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system monitoring logs or records; system audit records; system security plan; other relevant documents or records].
	SI-04(11)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system].

SI-04(11)	SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES	
	SI-04(11)-Test	[SELECT FROM: Organizational processes for intrusion detection and system monitoring; mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; mechanisms supporting and/or implementing the analysis of communications traffic].

SI-04(12)	SYSTEM MONITORING | AUTOMATED ORGANIZATION-GENERATED ALERTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(12)_ODP[01]	***personnel or roles to be alerted when indications of inappropriate or unusual activity with security or privacy implications occur is/are defined;***
	SI-04(12)_ODP[02]	***automated mechanisms used to alert personnel or roles are defined;***
	SI-04(12)_ODP[03]	***activities that trigger alerts to personnel or are defined;***
	SI-04(12)	***<SI-04(12)_ODP[01] personnel or roles>*** is/are alerted using ***<SI-04(12)_ODP[02] automated mechanisms>*** when ***<SI-04(12)_ODP[03] activities that trigger alerts>*** indicate inappropriate or unusual activities with security or privacy implications.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(12)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; list of inappropriate or unusual activities with security and privacy implications that trigger alerts; suspicious activity reports; alerts provided to security and privacy personnel; system monitoring logs or records; system audit records; system security plan; privacy plan; other relevant documents or records].
	SI-04(12)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; system developers; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system].
	SI-04(12)-Test	[SELECT FROM: Organizational processes for intrusion detection and system monitoring; automated mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; automated mechanisms supporting and/or implementing automated alerts to security personnel].

SI-04(13)	SYSTEM MONITORING | ANALYZE TRAFFIC AND EVENT PATTERNS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(13)(a)[01]	communications traffic for the system is analyzed;
	SI-04(13)(a)[02]	event patterns for the system are analyzed;
	SI-04(13)(b)[01]	profiles representing common traffic are developed;

SI-04(13)	SYSTEM MONITORING | ANALYZE TRAFFIC AND EVENT PATTERNS	
	SI-04(13)(b)[02]	profiles representing event patterns are developed;
	SI-04(13)(c)[01]	traffic profiles are used in tuning system-monitoring devices;
	SI-04(13)(c)[02]	event profiles are used in tuning system-monitoring devices.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(13)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; list of profiles representing common traffic patterns and/or events; system protocols documentation; list of acceptable thresholds for false positives and false negatives; system security plan; other relevant documents or records].
	SI-04(13)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system].
	SI-04(13)-Test	[SELECT FROM: Organizational processes for intrusion detection and system monitoring; mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; mechanisms supporting and/or implementing the analysis of communications traffic and event patterns].

SI-04(14)	SYSTEM MONITORING | WIRELESS INTRUSION DETECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(14)[01]	a wireless intrusion detection system is employed to identify rogue wireless devices;
	SI-04(14)[02]	a wireless intrusion detection system is employed to detect attack attempts on the system;
	SI-04(14)[03]	a wireless intrusion detection system is employed to detect potential compromises or breaches to the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(14)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system protocols; system audit records; system security plan; other relevant documents or records].
	SI-04(14)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system].

SI-04(14)	SYSTEM MONITORING | WIRELESS INTRUSION DETECTION	
	SI-04(14)-Test	[SELECT FROM: Organizational processes for intrusion detection; mechanisms supporting and/or implementing a wireless intrusion detection capability].

SI-04(15)	SYSTEM MONITORING | WIRELESS TO WIRELINE COMMUNICATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(15)	an intrusion detection system is employed to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(15)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system protocols documentation; system audit records; system security plan; other relevant documents or records].
	SI-04(15)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system].
	SI-04(15)-Test	[SELECT FROM: Organizational processes for intrusion detection and system monitoring; mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; mechanisms supporting and/or implementing a wireless intrusion detection capability].

SI-04(16)	SYSTEM MONITORING | CORRELATE MONITORING INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(16)	information from monitoring tools and mechanisms employed throughout the system is correlated.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(16)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; event correlation logs or records; system audit records; system security plan; other relevant documents or records].
	SI-04(16)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system].

SI-04(16)	SYSTEM MONITORING | CORRELATE MONITORING INFORMATION	
	SI-04(16)-Test	[SELECT FROM: Organizational processes for intrusion detection and system monitoring; mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; mechanisms supporting and/or implementing the correlation of information from monitoring tools].

SI-04(17)	SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(17)	information from monitoring physical, cyber, and supply chain activities are correlated to achieve integrated, organization-wide situational awareness.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(17)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; event correlation logs or records resulting from physical, cyber, and supply chain activities; system audit records; system security plan; supply chain risk management plan; other relevant documents or records].
	SI-04(17)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system].
	SI-04(17)-Test	[SELECT FROM: Organizational processes for intrusion detection and system monitoring; mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; mechanisms supporting and/or implementing the correlation of information from monitoring tools].

SI-04(18)	SYSTEM MONITORING | ANALYZE TRAFFIC AND COVERT EXFILTRATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(18)_ODP	***interior points within the system where communications traffic is to be analyzed are defined;***
	SI-04(18)[01]	outbound communications traffic is analyzed at interfaces external to the system to detect covert exfiltration of information;
	SI-04(18)[02]	outbound communications traffic is analyzed at ***<SI-04(18)_ODP interior points>*** to detect covert exfiltration of information.

SI-04(18)	SYSTEM MONITORING | ANALYZE TRAFFIC AND COVERT EXFILTRATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(18)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; network diagram; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system monitoring logs or records; system audit records; system security plan; other relevant documents or records].
	SI-04(18)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; organizational personnel responsible for the intrusion detection system].
	SI-04(18)-Test	[SELECT FROM: Organizational processes for intrusion detection and system monitoring; mechanisms supporting and/or implementing intrusion detection and system monitoring capabilities; mechanisms supporting and/or implementing an analysis of outbound communications traffic].

SI-04(19)	SYSTEM MONITORING | RISK FOR INDIVIDUALS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(19)_ODP[01]	***additional monitoring of individuals who have been identified as posing an increased level of risk is defined;***
	SI-04(19)_ODP[02]	***sources that identify individuals who pose an increased level of risk are defined;***
	SI-04(19)	***<SI-04(19)_ODP[01] additional monitoring>*** is implemented on individuals who have been identified by ***<SI-04(19)_ODP[02] sources>*** as posing an increased level of risk.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(19)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; other relevant documents or records].
	SI-04(19)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system; legal counsel; human resource officials; organizational personnel with personnel security responsibilities].
	SI-04(19)-Test	[SELECT FROM: Organizational processes for system monitoring; mechanisms supporting and/or implementing a system monitoring capability].

SI-04(20)	SYSTEM MONITORING | PRIVILEGED USERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(20)_ODP	***additional monitoring of privileged users is defined;***
	SI-04(20)	***<SI-04(20)_ODP additional monitoring>*** of privileged users is implemented.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(20)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system monitoring logs or records; system audit records; system security plan; other relevant documents or records].
	SI-04(20)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system].
	SI-04(20)-Test	[SELECT FROM: Organizational processes for system monitoring; mechanisms supporting and/or implementing a system monitoring capability].

SI-04(21)	SYSTEM MONITORING | PROBATIONARY PERIODS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(21)_ODP[01]	***additional monitoring to be implemented on individuals during probationary periods is defined;***
	SI-04(21)_ODP[02]	***the probationary period of individuals is defined;***
	SI-04(21)	***<SI-04(21)_ODP[01] additional monitoring>*** of individuals is implemented during ***<SI-04(21)_ODP[02] probationary period>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(21)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system monitoring logs or records; system audit records; system security plan; other relevant documents or records].
	SI-04(21)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system].
	SI-04(21)-Test	[SELECT FROM: Organizational processes for system monitoring; mechanisms supporting and/or implementing a system monitoring capability].

SI-04(22)	SYSTEM MONITORING | UNAUTHORIZED NETWORK SERVICES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(22)_ODP[01]	***authorization or approval processes for network services are defined;***
	SI-04(22)_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {audit; alert <SI-04(22)_ODP[03] personnel or roles>};***
	SI-04(22)_ODP[03]	***personnel or roles to be alerted upon the detection of network services that have not been authorized or approved by authorization or approval processes is/are defined (if selected);***
	SI-04(22)(a)	network services that have not been authorized or approved by ***<SI-04(22)_ODP[01] authorization or approval processes>*** are detected;
	SI-04(22)(b)	***<SI-04(22)_ODP[02] SELECTED PARAMETER VALUE(S)>*** is/are initiated when network services that have not been authorized or approved by authorization or approval processes are detected.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(22)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; documented authorization/approval of network services; notifications or alerts of unauthorized network services; system monitoring logs or records; system audit records; system security plan; other relevant documents or records].
	SI-04(22)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring the system].
	SI-04(22)-Test	[SELECT FROM: Organizational processes for system monitoring; mechanisms supporting and/or implementing a system monitoring capability; mechanisms for auditing network services; mechanisms for providing alerts].

SI-04(23)	SYSTEM MONITORING | HOST-BASED DEVICES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(23)_ODP[01]	***host-based monitoring mechanisms to be implemented on system components are defined;***
	SI-04(23)_ODP[02]	***system components where host-based monitoring is to be implemented are defined;***
	SI-04(23)	***<SI-04(23)_ODP[01] host-based monitoring mechanisms>*** are implemented on ***<SI-04(23)_ODP[02] system components>***.

SI-04(23)	SYSTEM MONITORING | HOST-BASED DEVICES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(23)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring tools and techniques; system design documentation; host-based monitoring mechanisms; system monitoring tools and techniques documentation; system configuration settings and associated documentation; list of system components requiring host-based monitoring; system monitoring logs or records; system audit records; system security plan; other relevant documents or records].
	SI-04(23)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring system hosts].
	SI-04(23)-Test	[SELECT FROM: Organizational processes for system monitoring; mechanisms supporting and/or implementing a host-based monitoring capability].

SI-04(24)	SYSTEM MONITORING | INDICATORS OF COMPROMISE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(24)_ODP[01]	***sources that provide indicators of compromise are defined;***
	SI-04(24)_ODP[02]	***personnel or roles to whom indicators of compromise are to be distributed is/are defined;***
	SI-04(24)[01]	indicators of compromise provided by ***<SI-04(24)_ODP[01] sources>*** are discovered;
	SI-04(24)[02]	indicators of compromise provided by ***<SI-04(24)_ODP[01] sources>*** are collected;
	SI-04(24)[03]	indicators of compromise provided by ***<SI-04(24)_ODP[01] sources>*** are distributed to ***<SI-04(24)_ODP[02] personnel or roles>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(24)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system monitoring logs or records; system audit records; system security plan; other relevant documents or records].
	SI-04(24)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring system hosts].
	SI-04(24)-Test	[SELECT FROM: Organizational processes for system monitoring; organizational processes for the discovery, collection, distribution, and use of indicators of compromise; mechanisms supporting and/or implementing a system monitoring capability; mechanisms supporting and/or implementing the discovery, collection, distribution, and use of indicators of compromise].

SI-04(25)	SYSTEM MONITORING | OPTIMIZE NETWORK TRAFFIC ANALYSIS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-04(25)[01]	visibility into network traffic at external system interfaces is provided to optimize the effectiveness of monitoring devices;
	SI-04(25)[02]	visibility into network traffic at key internal system interfaces is provided to optimize the effectiveness of monitoring devices.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-04(25)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system monitoring; system design documentation; system monitoring tools and techniques documentation; system configuration settings and associated documentation; system monitoring logs or records; system architecture; system audit records; network traffic reports; system security plan; other relevant documents or records].
	SI-04(25)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer; organizational personnel installing, configuring, and/or maintaining the system; organizational personnel responsible for monitoring system hosts].
	SI-04(25)-Test	[SELECT FROM: Organizational processes for system monitoring; organizational processes for the discovery, collection, distribution, and use of indicators of compromise; mechanisms supporting and/or implementing a system monitoring capability; mechanisms supporting and/or implementing the discovery, collection, distribution, and use of indicators of compromise].

SI-05	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-05_ODP[01]	***external organizations from whom system security alerts, advisories, and directives are to be received on an ongoing basis are defined;***
	SI-05_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {<SI-05_ODP[03] personnel or roles>; <SI-05_ODP[04] elements>; <SI-05_ODP[05] external organizations>};***
	SI-05_ODP[03]	***personnel or roles to whom security alerts, advisories, and directives are to be disseminated is/are defined (if selected);***
	SI-05_ODP[04]	***elements within the organization to whom security alerts, advisories, and directives are to be disseminated are defined (if selected);***
	SI-05_ODP[05]	***external organizations to whom security alerts, advisories, and directives are to be disseminated are defined (if selected);***
	SI-05a.	system security alerts, advisories, and directives are received from ***<SI-05_ODP[01] external organizations>*** on an ongoing basis;
	SI-05b.	internal security alerts, advisories, and directives are generated as deemed necessary;
	SI-05c.	security alerts, advisories, and directives are disseminated to ***<SI-05_ODP[02] SELECTED PARAMETER VALUE(S)>***;

SI-05	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	
	SI-05d.	security directives are implemented in accordance with established time frames or if the issuing organization is notified of the degree of noncompliance.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-05-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing security alerts, advisories, and directives; records of security alerts and advisories; system security plan; other relevant documents or records].
	SI-05-Interview	[SELECT FROM: Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, and using the system; organizational personnel, organizational elements, and/or external organizations to whom alerts, advisories, and directives are to be disseminated; system/network administrators; organizational personnel with information security responsibilities].
	SI-05-Test	[SELECT FROM: Organizational processes for defining, receiving, generating, disseminating, and complying with security alerts, advisories, and directives; mechanisms supporting and/or implementing the definition, receipt, generation, and dissemination of security alerts, advisories, and directives; mechanisms supporting and/or implementing security directives].

SI-05(01)	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-05(01)_ODP	***automated mechanisms used to broadcast security alert and advisory information throughout the organization are defined;***
	SI-05(01)	***<SI-05(01)_ODP automated mechanisms>*** are used to broadcast security alert and advisory information throughout the organization.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-05(01)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing security alerts, advisories, and directives; system design documentation; system configuration settings and associated documentation; automated mechanisms supporting the distribution of security alert and advisory information; records of security alerts and advisories; system audit records; system security plan; other relevant documents or records].
	SI-05(01)-Interview	[SELECT FROM: Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, and using the system; organizational personnel, organizational elements, and/or external organizations to whom alerts and advisories are to be disseminated; system/network administrators; organizational personnel with information security responsibilities].
	SI-05(01)-Test	[SELECT FROM: Organizational processes for defining, receiving, generating, and disseminating security alerts and advisories; automated mechanisms supporting and/or implementing the dissemination of security alerts and advisories].

SI-06	SECURITY AND PRIVACY FUNCTION VERIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-06_ODP[01]	***security functions to be verified for correct operation are defined;***
	SI-06_ODP[02]	***privacy functions to be verified for correct operation are defined;***
	SI-06_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {<SI-06_ODP[04] system transitional states>; upon command by user with appropriate privilege; <SI-06_ODP[05] frequency>};***
	SI-06_ODP[04]	***system transitional states requiring the verification of security and privacy functions are defined; (if selected)***
	SI-06_ODP[05]	***frequency at which to verify the correct operation of security and privacy functions is defined; (if selected)***
	SI-06_ODP[06]	***personnel or roles to be alerted of failed security and privacy verification tests is/are defined;***
	SI-06_ODP[07]	***one or more of the following PARAMETER VALUES is/are selected: {shut the system down; restart the system; <SI-06_ODP[08] alternative action(s)>};***
	SI-06_ODP[08]	***alternative action(s) to be performed when anomalies are discovered are defined (if selected);***
	SI-06a.[01]	***<SI-06_ODP[01] security functions>*** are verified to be operating correctly;
	SI-06a.[02]	***<SI-06_ODP[02] privacy functions>*** are verified to be operating correctly;
	SI-06b.[01]	***<SI-06_ODP[01] security functions>*** are verified ***<SI-06_ODP[03] SELECTED PARAMETER VALUE(S)>***;
	SI-06b.[02]	***<SI-06_ODP[02] privacy functions>*** are verified ***<SI-06_ODP[03] SELECTED PARAMETER VALUE(S)>***;
	SI-06c.[01]	***<SI-06_ODP[06] personnel or roles>*** is/are alerted to failed security verification tests;
	SI-06c.[02]	***<SI-06_ODP[06] personnel or roles>*** is/are alerted to failed privacy verification tests;
	SI-06d.	***<SI-06_ODP[07] SELECTED PARAMETER VALUE(S)>*** is/are initiated when anomalies are discovered.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-06-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing security and privacy function verification; system design documentation; system configuration settings and associated documentation; alerts/notifications of failed security verification tests; list of system transition states requiring security functionality verification; system audit records; system security plan; privacy plan; other relevant documents or records].
	SI-06-Interview	[SELECT FROM: Organizational personnel with security and privacy function verification responsibilities; organizational personnel implementing, operating, and maintaining the system; system/network administrators; organizational personnel with information security and privacy responsibilities; system developer].

SI-06	SECURITY AND PRIVACY FUNCTION VERIFICATION	
	SI-06-Test	[SELECT FROM: Organizational processes for security and privacy function verification; mechanisms supporting and/or implementing the security and privacy function verification capability].

SI-06(01)	SECURITY AND PRIVACY FUNCTION VERIFICATION | NOTIFICATION OF FAILED SECURITY TESTS	
	[WITHDRAWN: Incorporated into SI-06.]	

SI-06(02)	SECURITY AND PRIVACY FUNCTION VERIFICATION | AUTOMATION SUPPORT FOR DISTRIBUTED TESTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-06(02)[01]	automated mechanisms are implemented to support the management of distributed security function testing;
	SI-06(02)[02]	automated mechanisms are implemented to support the management of distributed privacy function testing.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-06(02)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing security and privacy function verification; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; other relevant documents or records].
	SI-06(02)-Interview	[SELECT FROM: Organizational personnel with security and privacy function verification responsibilities; organizational personnel implementing, operating, and maintaining the system; system/network administrators; organizational personnel with information security and privacy responsibilities].
	SI-06(02)-Test	[SELECT FROM: Organizational processes for security and privacy function verification; automated mechanisms supporting and/or implementing the management of distributed security and privacy testing].

SI-06(03)	SECURITY AND PRIVACY FUNCTION VERIFICATION | REPORT VERIFICATION RESULTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-06(03)_ODP	***personnel or roles designated to receive the results of security and privacy function verification is/are defined;***
	SI-06(03)[01]	the results of security function verification are reported to ***<SI-06(03)_ODP personnel or roles>***;
	SI-06(03)[02]	the results of privacy function verification are reported to ***<SI-06(03)_ODP personnel or roles>***.

SI-06(03)	SECURITY AND PRIVACY FUNCTION VERIFICATION | REPORT VERIFICATION RESULTS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-06(03)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing security and privacy function verification; system design documentation; system configuration settings and associated documentation; reports of security and privacy function verification results; system audit records; system security plan; privacy plan; other relevant documents or records].
	SI-06(03)-Interview	[SELECT FROM: Organizational personnel with security and privacy function verification responsibilities; organizational personnel who are recipients of security and privacy function verification reports; organizational personnel with information security and privacy responsibilities].
	SI-06(03)-Test	[SELECT FROM: Organizational processes for reporting security and privacy function verification results; mechanisms supporting and/or implementing the reporting of security and privacy function verification results].

SI-07	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-07_ODP[01]	***software requiring integrity verification tools to be employed to detect unauthorized changes is defined;***
	SI-07_ODP[02]	***firmware requiring integrity verification tools to be employed to detect unauthorized changes is defined;***
	SI-07_ODP[03]	***information requiring integrity verification tools to be employed to detect unauthorized changes is defined;***
	SI-07_ODP[04]	***actions to be taken when unauthorized changes to software are detected are defined;***
	SI-07_ODP[05]	***actions to be taken when unauthorized changes to firmware are detected are defined;***
	SI-07_ODP[06]	***actions to be taken when unauthorized changes to information are detected are defined;***
	SI-07a.[01]	integrity verification tools are employed to detect unauthorized changes to ***<SI-07_ODP[01] software>***;
	SI-07a.[02]	integrity verification tools are employed to detect unauthorized changes to ***<SI-07_ODP[02] firmware>***;
	SI-07a.[03]	integrity verification tools are employed to detect unauthorized changes to ***<SI-07_ODP[03] information>***;
	SI-07b.[01]	***<SI-07_ODP[04] actions>*** are taken when unauthorized changes to the software, are detected;
	SI-07b.[02]	***<SI-07_ODP[05] actions>*** are taken when unauthorized changes to the firmware are detected;
	SI-07b.[03]	***<SI-07_ODP[06] actions>*** are taken when unauthorized changes to the information are detected.

SI-07	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-07-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity; personally identifiable information processing policy; system design documentation; system configuration settings and associated documentation; integrity verification tools and associated documentation; records generated or triggered by integrity verification tools regarding unauthorized software, firmware, and information changes; system audit records; system security plan; privacy plan; other relevant documents or records].
	SI-07-Interview	[SELECT FROM: Organizational personnel responsible for software, firmware, and/or information integrity; organizational personnel with information security and privacy responsibilities; system/network administrators].
	SI-07-Test	[SELECT FROM: Software, firmware, and information integrity verification tools].

SI-07(01)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-07(01)_ODP[01]	***software on which an integrity check is to be performed is defined;***
	SI-07(01)_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {at startup; at <SI-07(01)_ODP[03] transitional states or security-relevant events>; <SI-07(01)_ODP[04] frequency>};***
	SI-07(01)_ODP[03]	***transitional states or security-relevant events requiring integrity checks (on software) are defined (if selected);***
	SI-07(01)_ODP[04]	***frequency with which to perform an integrity check (on software) is defined (if selected);***
	SI-07(01)_ODP[05]	***firmware on which an integrity check is to be performed is defined;***
	SI-07(01)_ODP[06]	***one or more of the following PARAMETER VALUES is/are selected: {at startup; at <SI-07(01)_ODP[07] transitional states or security-relevant events>; <SI-07(01)_ODP[08] frequency>};***
	SI-07(01)_ODP[07]	***transitional states or security-relevant events requiring integrity checks (on firmware) are defined (if selected);***
	SI-07(01)_ODP[08]	***frequency with which to perform an integrity check (on firmware) is defined (if selected);***
	SI-07(01)_ODP[09]	***information on which an integrity check is to be performed is defined;***
	SI-07(01)_ODP[10]	***one or more of the following PARAMETER VALUES is/are selected: {at startup; at <SI-07(01)_ODP[11] transitional states or security-relevant events>; <SI-07(01)_ODP[12] frequency>};***
	SI-07(01)_ODP[11]	***transitional states or security-relevant events requiring integrity checks (of information) are defined (if selected);***
	SI-07(01)_ODP[12]	***frequency with which to perform an integrity check (of information) is defined (if selected);***

SI-07(01)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS	
	SI-07(01)[01]	an integrity check of ***<SI-07(01)_ODP[01] software>*** is performed ***<SI-07(01)_ODP[02] SELECTED PARAMETER VALUE(S)>***;
	SI-07(01)[02]	an integrity check of ***<SI-07(01)_ODP[05] firmware>*** is performed ***<SI-07(01)_ODP[06] SELECTED PARAMETER VALUE(S)>***;
	SI-07(01)[03]	an integrity check of ***<SI-07(01)_ODP[09] information>*** is performed ***<SI-07(01)_ODP[10] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-07(01)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity testing; system design documentation; system configuration settings and associated documentation; integrity verification tools and associated documentation; records of integrity scans; system security plan; other relevant documents or records].
	SI-07(01)-Interview	[SELECT FROM: Organizational personnel responsible for software, firmware, and/or information integrity; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-07(01)-Test	[SELECT FROM: Software, firmware, and information integrity verification tools].

SI-07(02)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-07(02)_ODP	***personnel or roles to whom notification is to be provided upon discovering discrepancies during integrity verification is/are defined;***
	SI-07(02)	automated tools that provide notification to ***<SI-07(02)_ODP personnel or roles>*** upon discovering discrepancies during integrity verification are employed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-07(02)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity; personally identifiable information processing policy; system design documentation; system configuration settings and associated documentation; integrity verification tools and associated documentation; records of integrity scans; automated tools supporting alerts and notifications for integrity discrepancies; notifications provided upon discovering discrepancies during integrity verifications; system audit records; system security plan; privacy plan; other relevant documents or records].
	SI-07(02)-Interview	[SELECT FROM: Organizational personnel responsible for software, firmware, and/or information integrity; organizational personnel with information security and privacy responsibilities; system administrators; software developers].
	SI-07(02)-Test	[SELECT FROM: Software, firmware, and information integrity verification tools; mechanisms providing integrity discrepancy notifications].

SI-07(03)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CENTRALLY MANAGED INTEGRITY TOOLS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-07(03)	centrally managed integrity verification tools are employed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-07(03)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity; system design documentation; system configuration settings and associated documentation; integrity verification tools and associated documentation; records of integrity scans; system security plan; other relevant documents or records].
	SI-07(03)-Interview	[SELECT FROM: Organizational personnel responsible for the central management of integrity verification tools; organizational personnel with information security responsibilities].
	SI-07(03)-Test	[SELECT FROM: Mechanisms supporting and/or implementing the central management of integrity verification tools].

SI-07(04)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TAMPER-EVIDENT PACKAGING
	[WITHDRAWN: Incorporated into SR-09.]

SI-07(05)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-07(05)_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {shut down the system; restart the system; implement <SI-07(05)_ODP[02] controls>};***
	SI-07(05)_ODP[02]	***controls to be implemented automatically when integrity violations are discovered are defined (if selected);***
	SI-07(05)	***<SI-07(05)_ODP[01] SELECTED PARAMETER VALUE(S)>*** are automatically performed when integrity violations are discovered.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-07(05)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity; system design documentation; system configuration settings and associated documentation; integrity verification tools and associated documentation; records of integrity scans; records of integrity checks and responses to integrity violations; audit records; system security plan; other relevant documents or records].
	SI-07(05)-Interview	[SELECT FROM: Organizational personnel responsible for software, firmware, and/or information integrity; organizational personnel with information security responsibilities; system/network administrators; system developer].

SI-07(05)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS	
	SI-07(05)-Test	[SELECT FROM: Software, firmware, and information integrity verification tools; mechanisms providing an automated response to integrity violations; mechanisms supporting and/or implementing security safeguards to be implemented when integrity violations are discovered].

SI-07(06)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-07(06)[01]	cryptographic mechanisms are implemented to detect unauthorized changes to software;
	SI-07(06)[02]	cryptographic mechanisms are implemented to detect unauthorized changes to firmware;
	SI-07(06)[03]	cryptographic mechanisms are implemented to detect unauthorized changes to information.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-07(06)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms and associated documentation; records of detected unauthorized changes to software, firmware, and information; system audit records; system security plan; other relevant documents or records].
	SI-07(06)-Interview	[SELECT FROM: Organizational personnel responsible for software, firmware, and/or information integrity; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-07(06)-Test	[SELECT FROM: Software, firmware, and information integrity verification tools; cryptographic mechanisms implementing software, firmware, and information integrity].

SI-07(07)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-07(07)_ODP	***security-relevant changes to the system are defined;***
	SI-07(07)	the detection of ***<SI-07(07)_ODP changes>*** are incorporated into the organizational incident response capability.

SI-07(07)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-07(07)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity; procedures addressing incident response; system design documentation; system configuration settings and associated documentation; incident response records; audit records; system security plan; other relevant documents or records].
	SI-07(07)-Interview	[SELECT FROM: Organizational personnel responsible for software, firmware, and/or information integrity; organizational personnel with information security responsibilities; organizational personnel with incident response responsibilities].
	SI-07(07)-Test	[SELECT FROM: Organizational processes for incorporating the detection of unauthorized security-relevant changes into the incident response capability; software, firmware, and information integrity verification tools; mechanisms supporting and/or implementing the incorporation of detection of unauthorized security-relevant changes into the incident response capability].

SI-07(08)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUDITING CAPABILITY FOR SIGNIFICANT EVENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-07(08)_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {generate an audit record; alert current user; alert <SI-07(08)_ODP[02] personnel or roles>; <SI-07(08)_ODP[03] other actions>};***
	SI-07(08)_ODP[02]	***personnel or roles to be alerted upon the detection of a potential integrity violation is/are defined (if selected);***
	SI-07(08)_ODP[03]	***other actions to be taken upon the detection of a potential integrity violation are defined (if selected);***
	SI-07(08)[01]	the capability to audit an event upon the detection of a potential integrity violation is provided;
	SI-07(08)[02]	***<SI-07(08)_ODP[01] SELECTED PARAMETER VALUE(S)>*** is/are initiated upon the detection of a potential integrity violation.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-07(08)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity; system design documentation; system configuration settings and associated documentation; integrity verification tools and associated documentation; records of integrity scans; incident response records; list of security-relevant changes to the system; automated tools supporting alerts and notifications if unauthorized security changes are detected; system audit records; system security plan; other relevant documents or records].
	SI-07(08)-Interview	[SELECT FROM: Organizational personnel responsible for software, firmware, and/or information integrity; organizational personnel with information security responsibilities; system/network administrators; system developer].

SI-07(08)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUDITING CAPABILITY FOR SIGNIFICANT EVENTS	
	SI-07(08)-Test	[SELECT FROM: Software, firmware, and information integrity verification tools; mechanisms supporting and/or implementing the capability to audit potential integrity violations; mechanisms supporting and/or implementing alerts about potential integrity violations].

SI-07(09)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-07(09)_ODP	***system components requiring integrity verification of the boot process are defined;***
	SI-07(09)	the integrity of the boot process of ***<SI-07(09)_ODP system components>*** is verified.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-07(09)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity; system design documentation; system configuration settings and associated documentation; integrity verification tools and associated documentation; documentation; records of integrity verification scans; system audit records; system security plan; other relevant documents or records].
	SI-07(09)-Interview	[SELECT FROM: Organizational personnel responsible for software, firmware, and/or information integrity; organizational personnel with information security responsibilities; system developer].
	SI-07(09)-Test	[SELECT FROM: Software, firmware, and information integrity verification tools; mechanisms supporting and/or implementing integrity verification of the boot process].

SI-07(10)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-07(10)_ODP[01]	***mechanisms to be implemented to protect the integrity of boot firmware in system components are defined;***
	SI-07(10)_ODP[02]	***system components requiring mechanisms to protect the integrity of boot firmware are defined;***
	SI-07(10)	***<SI-07(10)_ODP[01] mechanisms>*** are implemented to protect the integrity of boot firmware in ***<SI-07(10)_ODP[02] system components>***.

SI-07(10)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-07(10)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity; system design documentation; system configuration settings and associated documentation; integrity verification tools and associated documentation; records of integrity verification scans; system audit records; system security plan; other relevant documents or records].
	SI-07(10)-Interview	[SELECT FROM: Organizational personnel responsible for software, firmware, and/or information integrity; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-07(10)-Test	[SELECT FROM: Software, firmware, and information integrity verification tools; mechanisms supporting and/or implementing protection of the integrity of boot firmware; safeguards implementing protection of the integrity of boot firmware].

SI-07(11)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES
	[WITHDRAWN: Moved to CM-07(06).]

SI-07(12)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY VERIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-07(12)_ODP	***user-installed software requiring integrity verification prior to execution is defined;***
	SI-07(12)	the integrity of ***<SI-07(12)_ODP user-installed software>*** is verified prior to execution.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-07(12)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity; system design documentation; system configuration settings and associated documentation; integrity verification records; system audit records; system security plan; other relevant documents or records].
	SI-07(12)-Interview	[SELECT FROM: Organizational personnel responsible for software, firmware, and/or information integrity; organizational personnel with information security responsibilities].
	SI-07(12)-Test	[SELECT FROM: Software, firmware, and information integrity verification tools; mechanisms supporting and/or implementing verification of the integrity of user-installed software prior to execution].

SI-07(13)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS
	[WITHDRAWN: Moved to CM-07(07).]

SI-07(14)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE
	[WITHDRAWN: Moved to CM-07(08).]

SI-07(15)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-07(15)_ODP	***software or firmware components to be authenticated by cryptographic mechanisms prior to installation are defined;***
	SI-07(15)	cryptographic mechanisms are implemented to authenticate ***<SI-07(15)_ODP software or firmware components>*** prior to installation.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-07(15)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software, firmware, and information integrity; system design documentation; system configuration settings and associated documentation; cryptographic mechanisms and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-07(15)-Interview	[SELECT FROM: Organizational personnel responsible for software, firmware, and/or information integrity; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-07(15)-Test	[SELECT FROM: Cryptographic mechanisms authenticating software and firmware prior to installation].

SI-07(16)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-07(16)_ODP	***the maximum time period permitted for processes to execute without supervision is defined;***
	SI-07(16)	processes are prohibited from executing without supervision for more than ***<SI-07(16)_ODP time period>***.

SI-07(16)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-07(16)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software and information integrity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-07(16)-Interview	[SELECT FROM: Organizational personnel responsible for software, firmware, and/or information integrity; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-07(16)-Test	[SELECT FROM: Software, firmware, and information integrity verification tools; mechanisms supporting and/or implementing time limits on process execution without supervision].

SI-07(17)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | RUNTIME APPLICATION SELF-PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-07(17)_ODP	***controls to be implemented for application self-protection at runtime are defined;***
	SI-07(17)	***<SI-07(17)_ODP controls>*** are implemented for application self-protection at runtime.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-07(17)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing software and information integrity; system design documentation; system configuration settings and associated documentation; list of known vulnerabilities addressed by runtime instrumentation; system security plan; other relevant documents or records].
	SI-07(17)-Interview	[SELECT FROM: Organizational personnel responsible for software, firmware, and/or information integrity; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-07(17)-Test	[SELECT FROM: Software, firmware, and information integrity verification tools; mechanisms supporting and/or implementing runtime application self-protection].

SI-08	SPAM PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-08a.[01]	spam protection mechanisms are employed at system entry points to detect unsolicited messages;
	SI-08a.[02]	spam protection mechanisms are employed at system exit points to detect unsolicited messages;

SI-08	SPAM PROTECTION	
	SI-08a.[03]	spam protection mechanisms are employed at system entry points to act on unsolicited messages;
	SI-08a.[04]	spam protection mechanisms are employed at system exit points to act on unsolicited messages;
	SI-08b.	spam protection mechanisms are updated when new releases are available in accordance with organizational configuration management policies and procedures.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-08-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; configuration management policies and procedures (CM-01); procedures addressing spam protection; spam protection mechanisms; records of spam protection updates; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-08-Interview	[SELECT FROM: Organizational personnel responsible for spam protection; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-08-Test	[SELECT FROM: Organizational processes for implementing spam protection; mechanisms supporting and/or implementing spam protection].

SI-08(01)	SPAM PROTECTION | CENTRAL MANAGEMENT	
	[WITHDRAWN: Incorporated into PL-09.]	

SI-08(02)	SPAM PROTECTION | AUTOMATIC UPDATES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-08(02)_ODP	***the frequency at which to automatically update spam protection mechanisms is defined;***
	SI-08(02)	spam protection mechanisms are automatically updated ***<SI-08(02)_ODP frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-08(02)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing spam protection; spam protection mechanisms; records of spam protection updates; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-08(02)-Interview	[SELECT FROM: Organizational personnel responsible for spam protection; organizational personnel with information security responsibilities; system/network administrators; system developer].

SI-08(02)	SPAM PROTECTION | AUTOMATIC UPDATES	
	SI-08(02)-Test	[SELECT FROM: Organizational processes for spam protection; mechanisms supporting and/or implementing automatic updates to spam protection mechanisms].

SI-08(03)	SPAM PROTECTION | CONTINUOUS LEARNING CAPABILITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-08(03)	spam protection mechanisms with a learning capability are implemented to more effectively identify legitimate communications traffic.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-08(03)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing spam protection; spam protection mechanisms; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-08(03)-Interview	[SELECT FROM: Organizational personnel responsible for spam protection; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-08(03)-Test	[SELECT FROM: Organizational processes for spam protection; mechanisms supporting and/or implementing spam protection mechanisms with a learning capability].

SI-09	INFORMATION INPUT RESTRICTIONS
	[WITHDRAWN: Incorporated into AC-02, AC-03, AC-05, AC-06.]

SI-10	INFORMATION INPUT VALIDATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-10_ODP	***information inputs to the system requiring validity checks are defined;***
	SI-10	the validity of the ***<SI-10_ODP information inputs>*** is checked.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-10-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; access control policy and procedures; separation of duties policy and procedures; procedures addressing information input validation; documentation for automated tools and applications to verify the validity of information; list of information inputs requiring validity checks; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].

SI-10	INFORMATION INPUT VALIDATION	
	SI-10-Interview	[SELECT FROM: Organizational personnel responsible for information input validation; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-10-Test	[SELECT FROM: Mechanisms supporting and/or implementing validity checks on information inputs].

SI-10(01)	INFORMATION INPUT VALIDATION | MANUAL OVERRIDE CAPABILITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-10(01)_ODP	***authorized individuals who can use the manual override capability are defined;***
	SI-10(01)(a)	a manual override capability for the validation of ***<SI-10_ODP information inputs>*** is provided;
	SI-10(01)(b)	the use of the manual override capability is restricted to only ***<SI-10(01)_ODP authorized individuals>***;
	SI-10(01)(c)	the use of the manual override capability is audited.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-10(01)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; access control policy and procedures; separation of duties policy and procedures; procedures addressing information input validation; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-10(01)-Interview	[SELECT FROM: Organizational personnel responsible for information input validation; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-10(01)-Test	[SELECT FROM: Organizational processes for the use of a manual override capability; mechanisms supporting and/or implementing a manual override capability for input validation; mechanisms supporting and/or implementing auditing of the use of a manual override capability].

SI-10(02)	INFORMATION INPUT VALIDATION | REVIEW AND RESOLVE ERRORS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-10(02)_ODP[01]	***the time period within which input validation errors are to be reviewed is defined;***
	SI-10(02)_ODP[02]	***the time period within which input validation errors are to be resolved is defined;***
	SI-10(02)[01]	input validation errors are reviewed within ***<SI-10(02)_ODP[01] time period>***;
	SI-10(02)[02]	input validation errors are resolved within ***<SI-10(02)_ODP[02] time period>***.

SI-10(02)	INFORMATION INPUT VALIDATION | REVIEW AND RESOLVE ERRORS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-10(02)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing information input validation; system design documentation; system configuration settings and associated documentation; review records of information input validation errors and resulting resolutions; information input validation error logs or records; system audit records; system security plan; other relevant documents or records].
	SI-10(02)-Interview	[SELECT FROM: Organizational personnel responsible for information input validation; organizational personnel with information security responsibilities; system/network administrators].
	SI-10(02)-Test	[SELECT FROM: Organizational processes for the review and resolution of input validation errors; mechanisms supporting and/or implementing the review and resolution of input validation errors].

SI-10(03)	INFORMATION INPUT VALIDATION | PREDICTABLE BEHAVIOR	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-10(03)[01]	the system behaves in a predictable manner when invalid inputs are received;
	SI-10(03)[02]	the system behaves in a documented manner when invalid inputs are received.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-10(03)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing information input validation; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-10(03)-Interview	[SELECT FROM: Organizational personnel responsible for information input validation; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-10(03)-Test	[SELECT FROM: Automated mechanisms supporting and/or implementing predictable behavior when invalid inputs are received].

SI-10(04)	INFORMATION INPUT VALIDATION | TIMING INTERACTIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-10(04)	timing interactions among system components are accounted for in determining appropriate responses for invalid inputs.

SI-10(04)	INFORMATION INPUT VALIDATION | TIMING INTERACTIONS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-10(04)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing information input validation; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-10(04)-Interview	[SELECT FROM: Organizational personnel responsible for information input validation; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-10(04)-Test	[SELECT FROM: Organizational processes for determining appropriate responses to invalid inputs; automated mechanisms supporting and/or implementing responses to invalid inputs].

SI-10(05)	INFORMATION INPUT VALIDATION | RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-10(05)_ODP[01]	***trusted sources to which the use of information inputs is to be restricted are defined;***
	SI-10(05)_ODP[02]	***formats to which the use of information inputs is to be restricted are defined;***
	SI-10(05)	the use of information inputs is restricted to ***<SI-10(05)_ODP[01] trusted sources>*** and/or ***<SI-10(05)_ODP[02] formats>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-10(05)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing information input validation; system design documentation; system configuration settings and associated documentation; list of trusted sources for information inputs; list of acceptable formats for input restrictions; system audit records; system security plan; other relevant documents or records].
	SI-10(05)-Interview	[SELECT FROM: Organizational personnel responsible for information input validation; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-10(05)-Test	[SELECT FROM: Organizational processes for restricting information inputs; automated mechanisms supporting and/or implementing restriction of information inputs].

SI-10(06)	INFORMATION INPUT VALIDATION | INJECTION PREVENTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-10(06)	untrusted data injections are prevented.

SI-10(06)	INFORMATION INPUT VALIDATION | INJECTION PREVENTION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-10(06)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing information input validation; system design documentation; system configuration settings and associated documentation; list of trusted sources for information inputs; list of acceptable formats for input restrictions; system audit records; system security plan; other relevant documents or records].
	SI-10(06)-Interview	[SELECT FROM: Organizational personnel responsible for information input validation; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-10(06)-Test	[SELECT FROM: Organizational processes for preventing untrusted data injections; automated mechanisms supporting and/or implementing injection prevention].

SI-11	ERROR HANDLING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-11_ODP	***personnel or roles to whom error messages are to be revealed is/are defined;***
	SI-11a.	error messages that provide the information necessary for corrective actions are generated without revealing information that could be exploited;
	SI-11b.	error messages are revealed only to ***<SI-11_ODP personnel or roles>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-11-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing system error handling; system design documentation; system configuration settings and associated documentation; documentation providing the structure and content of error messages; system audit records; system security plan; other relevant documents or records].
	SI-11-Interview	[SELECT FROM: Organizational personnel responsible for information input validation; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-11-Test	[SELECT FROM: Organizational processes for error handling; automated mechanisms supporting and/or implementing error handling; automated mechanisms supporting and/or implementing the management of error messages].

SI-12	INFORMATION MANAGEMENT AND RETENTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-12[01]	information within the system is managed in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements;

SI-12	INFORMATION MANAGEMENT AND RETENTION	
	SI-12[02]	information within the system is retained in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements;
	SI-12[03]	information output from the system is managed in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements;
	SI-12[04]	information output from the system is retained in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-12-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; records retention and disposition policy; records retention and disposition procedures; federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements applicable to information management and retention; media protection policy; media protection procedures; audit findings; system security plan; privacy plan; privacy program plan; personally identifiable information inventory; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SI-12-Interview	[SELECT FROM: Organizational personnel with information and records management, retention, and disposition responsibilities; organizational personnel with information security and privacy responsibilities; network administrators].
	SI-12-Test	[SELECT FROM: Organizational processes for information management, retention, and disposition; automated mechanisms supporting and/or implementing information management, retention, and disposition].

SI-12(01)	INFORMATION MANAGEMENT AND RETENTION | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-12(01)_ODP	***elements of personally identifiable information being processed in the information life cycle are defined;***
	SI-12(01)	personally identifiable information being processed in the information life cycle is limited to ***<SI-12(01)_ODP elements of personally identifiable information>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-12(01)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; personally identifiable information processing procedures; records retention and disposition policy; records retention and disposition procedures; federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements applicable to limiting personally identifiable information elements; personally identifiable information inventory; system audit records; audit findings; system security plan; privacy plan; privacy program plan; privacy impact assessment; privacy risk assessment documentation; data mapping documentation; other relevant documents or records].

SI-12(01)	INFORMATION MANAGEMENT AND RETENTION | LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS	
	SI-12(01)-Interview	[SELECT FROM: Organizational personnel with information and records management, retention, and disposition responsibilities; organizational personnel with security and privacy responsibilities; network administrators].
	SI-12(01)-Test	[SELECT FROM: Organizational processes for information management and retention (including limiting personally identifiable information processing); automated mechanisms supporting and/or implementing limits to personally identifiable information processing].

SI-12(02)	INFORMATION MANAGEMENT AND RETENTION | MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-12(02)_ODP[01]	***techniques used to minimize the use of personally identifiable information for research are defined;***
	SI-12(02)_ODP[02]	***techniques used to minimize the use of personally identifiable information for testing are defined;***
	SI-12(02)_ODP[03]	***techniques used to minimize the use of personally identifiable information for training are defined;***
	SI-12(02)[01]	***<SI-12(02)_ODP[01] techniques>*** are used to minimize the use of personally identifiable information for research;
	SI-12(02)[02]	***<SI-12(02)_ODP[02] techniques>*** are used to minimize the use of personally identifiable information for testing;
	SI-12(02)[03]	***<SI-12(02)_ODP[03] techniques>*** are used to minimize the use of personally identifiable information for training.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-12(02)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; personally identifiable information processing procedures; federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements applicable to minimizing the use of personally identifiable information in testing, training, and research; policy for the minimization of personally identifiable information used in testing, training, and research; procedures for the minimization of personally identifiable information used in testing, training, and research; documentation supporting minimization policy implementation (e.g., templates for testing, training, and research); data sets used for testing, training, and research; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SI-12(02)-Interview	[SELECT FROM: Organizational personnel with information and records management, retention, and disposition responsibilities; organizational personnel with information security and privacy responsibilities; network administrators; system developers; personnel with IRB responsibilities].

SI-12(02)	INFORMATION MANAGEMENT AND RETENTION | MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH	
	SI-12(02)-Test	[SELECT FROM: Organizational processes for the minimization of personally identifiable information used in testing, training, and research; automated mechanisms supporting and/or implementing the minimization of personally identifiable information used in testing, training, and research].

SI-12(03)	INFORMATION MANAGEMENT AND RETENTION | INFORMATION DISPOSAL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-12(03)_ODP[01]	***techniques used to dispose of information following the retention period are defined;***
	SI-12(03)_ODP[02]	***techniques used to destroy information following the retention period are defined;***
	SI-12(03)_ODP[03]	***techniques used to erase information following the retention period are defined;***
	SI-12(03)[01]	***<SI-12(03)_ODP[01] techniques>*** are used to dispose of information following the retention period;
	SI-12(03)[02]	***<SI-12(03)_ODP[02] techniques>*** are used to destroy information following the retention period;
	SI-12(03)[03]	***<SI-12(03)_ODP[03] techniques>*** are used to erase information following the retention period.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-12(03)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; personally identifiable information processing procedures; records retention and disposition policy; records retention and disposition procedures; laws, Executive Orders, directives, policies, regulations, standards, and operational requirements applicable to information disposal; media protection policy; media protection procedures; system audit records; audit findings; information disposal records; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SI-12(03)-Interview	[SELECT FROM: Organizational personnel with information and records management, retention, and disposition responsibilities; organizational personnel with information security and privacy responsibilities; network administrators].
	SI-12(03)-Test	[SELECT FROM: Organizational processes for information disposition; automated mechanisms supporting and/or implementing information disposition].

SI-13	PREDICTABLE FAILURE PREVENTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-13_ODP[01]	***system components for which mean time to failure (MTTF) should be determined are defined;***

SI-13	PREDICTABLE FAILURE PREVENTION	
	SI-13_ODP[02]	***mean time to failure (MTTF) substitution criteria to be used as a means to exchange active and standby components are defined;***
	SI-13a.	mean time to failure (MTTF) is determined for ***<SI-13_ODP[01] system components>*** in specific environments of operation;
	SI-13b.	substitute system components and a means to exchange active and standby components are provided in accordance with ***<SI-13_ODP[02] mean time to failure (MTTF) substitution criteria>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-13-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing predictable failure prevention; system design documentation; system configuration settings and associated documentation; list of MTTF substitution criteria; system audit records; system security plan; other relevant documents or records].
	SI-13-Interview	[SELECT FROM: Organizational personnel responsible for MTTF determinations and activities; organizational personnel with information security responsibilities; system/network administrators; organizational personnel with contingency planning responsibilities].
	SI-13-Test	[SELECT FROM: Organizational processes for managing MTTF].

SI-13(01)	PREDICTABLE FAILURE PREVENTION | TRANSFERRING COMPONENT RESPONSIBILITIES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-13(01)_ODP	***the fraction or percentage of mean time to failure within which to transfer the responsibilities of a system component to a substitute component is defined;***
	SI-13(01)	system components are taken out of service by transferring component responsibilities to substitute components no later than ***<SI-13(01)_ODP fraction or percentage>*** of mean time to failure.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-13(01)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing predictable failure prevention; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-13(01)-Interview	[SELECT FROM: Organizational personnel responsible for MTTF activities; organizational personnel with information security responsibilities; system/network administrators; organizational personnel with contingency planning responsibilities].
	SI-13(01)-Test	[SELECT FROM: Organizational processes for managing MTTF; automated mechanisms supporting and/or implementing the transfer of component responsibilities to substitute components].

SI-13(02)	PREDICTABLE FAILURE PREVENTION | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION
	[WITHDRAWN: Incorporated into SI-07(16).]

SI-13(03)	PREDICTABLE FAILURE PREVENTION | MANUAL TRANSFER BETWEEN COMPONENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-13(03)_ODP	***the percentage of the mean time to failure for transfers to be manually initiated is defined;***
	SI-13(03)	transfers are initiated manually between active and standby system components when the use of the active component reaches ***<SI-13(03)_ODP percentage>*** of the mean time to failure.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-13(03)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing predictable failure prevention; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-13(03)-Interview	[SELECT FROM: Organizational personnel responsible for MTTF activities; organizational personnel with information security responsibilities; system/network administrators; organizational personnel with contingency planning responsibilities].
	SI-13(03)-Test	[SELECT FROM: Organizational processes for managing MTTF and conducting the manual transfer between active and standby components].

SI-13(04)	PREDICTABLE FAILURE PREVENTION | STANDBY COMPONENT INSTALLATION AND NOTIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-13(04)_ODP[01]	***time period for standby components to be installed is defined;***
	SI-13(04)_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {activate <SI-13(04)_ODP[03] alarm>; automatically shut down the system; <SI-13(04)_ODP[04] action>};***
	SI-13(04)_ODP[03]	***alarm to be activated when system component failures are detected is defined (if selected);***
	SI-13(04)_ODP[04]	***action to be taken when system component failures are detected is defined (if selected);***
	SI-13(04)(a)	the standby components are successfully and transparently installed within ***<SI-13(04)_ODP[01] time period>*** if system component failures are detected;
	SI-13(04)(b)	***<SI-13(04)_ODP[02] SELECTED PARAMETER VALUE(S)>*** are performed if system component failures are detected.

SI-13(04)	PREDICTABLE FAILURE PREVENTION | STANDBY COMPONENT INSTALLATION AND NOTIFICATION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-13(04)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing predictable failure prevention; system design documentation; system configuration settings and associated documentation; list of actions to be taken once system component failure is detected; system audit records; system security plan; other relevant documents or records].
	SI-13(04)-Interview	[SELECT FROM: Organizational personnel responsible for MTTF activities; organizational personnel with information security responsibilities; system/network administrators; organizational personnel with contingency planning responsibilities].
	SI-13(04)-Test	[SELECT FROM: Organizational processes for managing MTTF; automated mechanisms supporting and/or implementing the transparent installation of standby components; automated mechanisms supporting and/or implementing alarms or system shutdown if component failures are detected].

SI-13(05)	PREDICTABLE FAILURE PREVENTION | FAILOVER CAPABILITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-13(05)_ODP[01]	***one of the following PARAMETER VALUES is selected: {real-time; near real-time};***
	SI-13(05)_ODP[02]	***a failover capability for the system has been defined;***
	SI-13(05)	***<SI-13(05)_ODP[01] SELECTED PARAMETER VALUE> <SI-13(05)_ODP[02] failover capability>*** is provided for the system.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-13(05)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing predictable failure prevention; system design documentation; system configuration settings and associated documentation; documentation describing the failover capability provided for the system; system audit records; system security plan; other relevant documents or records].
	SI-13(05)-Interview	[SELECT FROM: Organizational personnel responsible for the failover capability; organizational personnel with information security responsibilities; system/network administrators; organizational personnel with contingency planning responsibilities].
	SI-13(05)-Test	[SELECT FROM: Organizational processes for managing the failover capability; automated mechanisms supporting and/or implementing the failover capability].

SI-14	NON-PERSISTENCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-14_ODP[01]	***non-persistent system components and services to be implemented are defined;***
	SI-14_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {upon end of session of use; <SI-14_ODP[03] frequency>};***
	SI-14_ODP[03]	***the frequency at which to terminate non-persistent components and services that are initiated in a known state is defined (if selected);***
	SI-14[01]	non-persistent ***<SI-14_ODP[01] system components and services>*** that are initiated in a known state are implemented;
	SI-14[02]	non-persistent ***<SI-14_ODP[01] system components and services>*** are terminated ***<SI-14_ODP[02] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-14-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing non-persistence for system components; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-14-Interview	[SELECT FROM: Organizational personnel responsible for non-persistence; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-14-Test	[SELECT FROM: Automated mechanisms supporting and/or implementing the initiation and termination of non-persistent components].

SI-14(01)	NON-PERSISTENCE | REFRESH FROM TRUSTED SOURCES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-14(01)_ODP	***trusted sources to obtain software and data for system component and service refreshes are defined;***
	SI-14(01)	the software and data employed during system component and service refreshes are obtained from ***<SI-14(01)_ODP trusted sources>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-14(01)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing non-persistence for system components; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-14(01)-Interview	[SELECT FROM: Organizational personnel responsible for obtaining component and service refreshes from trusted sources; organizational personnel with information security responsibilities].

SI-14(01)	NON-PERSISTENCE | REFRESH FROM TRUSTED SOURCES	
	SI-14(01)-Test	[SELECT FROM: Organizational processes for defining and obtaining component and service refreshes from trusted sources; automated mechanisms supporting and/or implementing component and service refreshes].

SI-14(02)	NON-PERSISTENCE | NON-PERSISTENT INFORMATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-14(02)_ODP[01]	***one of the following PARAMETER VALUES is selected: {refresh <SI-14(02)_ODP[02] information> <SI-14(02)_ODP[03] frequency>; generate <SI-14(02)_ODP[04] information> on demand};***
	SI-14(02)_ODP[02]	***the information to be refreshed is defined (if selected);***
	SI-14(02)_ODP[03]	***the frequency at which to refresh information is defined (if selected);***
	SI-14(02)_ODP[04]	***the information to be generated is defined (if selected);***
	SI-14(02)(a)	***<SI-14(02)_ODP[01] SELECTED PARAMETER VALUE>*** is performed;
	SI-14(02)(b)	information is deleted when no longer needed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-14(02)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing non-persistence for system components; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-14(02)-Interview	[SELECT FROM: Organizational personnel responsible for ensuring that information is and remains non-persistent; organizational personnel with information security responsibilities].
	SI-14(02)-Test	[SELECT FROM: Organizational processes for ensuring that information is and remains non-persistent; automated mechanisms supporting and/or implementing component and service refreshes].

SI-14(03)	NON-PERSISTENCE | NON-PERSISTENT CONNECTIVITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-14(03)_ODP	***one of the following PARAMETER VALUES is selected: {completion of a request; a period of non-use};***
	SI-14(03)[01]	connections to the system are established on demand;
	SI-14(03)[02]	connections to the system are terminated after ***<SI-14(03)_ODP SELECTED PARAMETER VALUE>***.

SI-14(03)	NON-PERSISTENCE | NON-PERSISTENT CONNECTIVITY	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-14(03)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing non-persistence for system components; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-14(03)-Interview	[SELECT FROM: Organizational personnel responsible for limiting persistent connections; organizational personnel with information security responsibilities].
	SI-14(03)-Test	[SELECT FROM: Organizational processes for limiting persistent connections; automated mechanisms supporting and/or implementing non-persistent connectivity].

SI-15	INFORMATION OUTPUT FILTERING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-15_ODP	***software programs and/or applications whose information output requires validation are defined;***
	SI-15	information output from ***<SI-15_ODP software programs and/or applications>*** is validated to ensure that the information is consistent with the expected content.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-15-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing information output filtering; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SI-15-Interview	[SELECT FROM: Organizational personnel responsible for validating information output; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-15-Test	[SELECT FROM: Organizational processes for validating information output; automated mechanisms supporting and/or implementing information output validation].

SI-16	MEMORY PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-16_ODP	***controls to be implemented to protect the system memory from unauthorized code execution are defined;***
	SI-16	***<SI-16_ODP controls>*** are implemented to protect the system memory from unauthorized code execution.

SI-16	MEMORY PROTECTION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-16-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; procedures addressing memory protection for the system; system design documentation; system configuration settings and associated documentation; list of security safeguards protecting system memory from unauthorized code execution; system audit records; system security plan; other relevant documents or records].
	SI-16-Interview	[SELECT FROM: Organizational personnel responsible for memory protection; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-16-Test	[SELECT FROM: Automated mechanisms supporting and/or implementing safeguards to protect the system memory from unauthorized code execution].

SI-17	FAIL-SAFE PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-17_ODP[01]	***fail-safe procedures associated with failure conditions are defined;***
	SI-17_ODP[02]	***a list of failure conditions requiring fail-safe procedures is defined;***
	SI-17	***<SI-17_ODP[01] fail-safe procedures>*** are implemented when ***<SI-17_ODP[02] list of failure conditions>*** occur.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-17-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; documentation addressing fail-safe procedures for the system; system design documentation; system configuration settings and associated documentation; list of security safeguards protecting the system memory from unauthorized code execution; system audit records; system security plan; other relevant documents or records].
	SI-17-Interview	[SELECT FROM: Organizational personnel responsible for fail-safe procedures; organizational personnel with information security responsibilities; system/network administrators; system developer].
	SI-17-Test	[SELECT FROM: Organizational fail-safe procedures; automated mechanisms supporting and/or implementing fail-safe procedures].

SI-18	PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-18_ODP[01]	***the frequency at which to check the accuracy of personally identifiable information across the information life cycle is defined;***
	SI-18_ODP[02]	***the frequency at which to check the relevance of personally identifiable information across the information life cycle is defined;***

SI-18	PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS	
	SI-18_ODP[03]	***the frequency at which to check the timeliness of personally identifiable information across the information life cycle is defined;***
	SI-18_ODP[04]	***the frequency at which to check the completeness of personally identifiable information across the information life cycle is defined;***
	SI-18a.[01]	the accuracy of personally identifiable information across the information life cycle is checked ***<SI-18_ODP[01] frequency>***;
	SI-18a.[02]	the relevance of personally identifiable information across the information life cycle is checked ***<SI-18_ODP[02] frequency>***;
	SI-18a.[03]	the timeliness of personally identifiable information across the information life cycle is checked ***<SI-18_ODP[03] frequency>***;
	SI-18a.[04]	the completeness of personally identifiable information across the information life cycle is checked ***<SI-18_ODP[04] frequency>***;
	SI-18b.	inaccurate or outdated personally identifiable information is corrected or deleted.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-18-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; documentation addressing personally identifiable information quality operations; quality reports; maintenance logs; system audit records; audit findings; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SI-18-Interview	[SELECT FROM: Organizational personnel responsible for performing personally identifiable information quality inspections; organizational personnel with information security responsibilities; organizational personnel with privacy responsibilities].
	SI-18-Test	[SELECT FROM: Organizational processes for personally identifiable information quality inspection; automated mechanisms supporting and/or implementing personally identifiable information quality operations].

SI-18(01)	PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS | AUTOMATION SUPPORT	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-18(01)_ODP	***automated mechanisms used to correct or delete personally identifiable information that is inaccurate, outdated, incorrectly determined regarding impact, or incorrectly de-identified are defined;***
	SI-18(01)	***<SI-18(01)_ODP automated mechanisms>*** are used to correct or delete personally identifiable information that is inaccurate, outdated, incorrectly determined regarding impact, or incorrectly de-identified.

SI-18(01)	PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS | AUTOMATION SUPPORT	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-18(01)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; documentation addressing personally identifiable information quality operations; quality reports; maintenance logs; system audit records; audit findings; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SI-18(01)-Interview	[SELECT FROM: Organizational personnel responsible for performing personally identifiable information quality inspections; organizational personnel with information security and privacy responsibilities].
	SI-18(01)-Test	[SELECT FROM: Organizational processes for personally identifiable information quality inspection; automated mechanisms supporting and/or implementing personally identifiable information quality operations].

SI-18(02)	PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS | DATA TAGS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-18(02)	data tags are employed to automate the correction or deletion of personally identifiable information across the information life cycle within organizational systems.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-18(02)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; procedures addressing data tagging; personally identifiable information inventory; system audit records; audit findings; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SI-18(02)-Interview	[SELECT FROM: Organizational personnel responsible for tagging data; organizational personnel with information security and privacy responsibilities].
	SI-18(02)-Test	[SELECT FROM: Data tagging mechanisms; automated mechanisms supporting and/or implementing data tagging].

SI-18(03)	PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS | COLLECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-18(03)	personally identifiable information is collected directly from the individual.

SI-18(03)	PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS | COLLECTION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-18(03)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; system configuration documentation; system audit records; user interface where personally identifiable information is collected; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SI-18(03)-Interview	[SELECT FROM: Organizational personnel responsible for data collection; organizational personnel with information security and privacy responsibilities].
	SI-18(03)-Test	[SELECT FROM: Data collection mechanisms; automated mechanisms supporting and/or validating collection directly from the individual].

SI-18(04)	PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS | INDIVIDUAL REQUESTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-18(04)	personally identifiable information is corrected or deleted upon request by individuals or their designated representatives.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-18(04)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; system configuration; individual requests; records of correction or deletion actions performed; system audit records; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SI-18(04)-Interview	[SELECT FROM: Organizational personnel responsible for responding to individual requests for personally identifiable information correction or deletion; organizational personnel with information security and privacy responsibilities].
	SI-18(04)-Test	[SELECT FROM: Request mechanisms; automated mechanisms supporting and/or implementing individual requests for correction or deletion].

SI-18(05)	PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS | NOTICE OF CORRECTION OR DELETION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-18(05)_ODP	***recipients of personally identifiable information to be notified when the personally identifiable information has been corrected or deleted are defined;***
	SI-18(05)	***<SI-18(05)_ODP recipients>*** and individuals are notified when the personally identifiable information has been corrected or deleted.

SI-18(05)	PERSONALLY IDENTIFIABLE INFORMATION QUALITY OPERATIONS | NOTICE OF CORRECTION OR DELETION	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-18(05)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; system configuration; individual requests for corrections or deletions; notifications of correction or deletion action; system audit records; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SI-18(05)-Interview	[SELECT FROM: Organizational personnel responsible for sending correction or deletion notices; organizational personnel with information security and privacy responsibilities].
	SI-18(05)-Test	[SELECT FROM: Organizational processes for notifications of correction or deletion; automated mechanisms supporting and/or implementing notifications of correction or deletion].

SI-19	DE-IDENTIFICATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-19_ODP[01]	***elements of personally identifiable information to be removed from datasets are defined;***
	SI-19_ODP[02]	***the frequency at which to evaluate the effectiveness of de-identification is defined;***
	SI-19a.	***<SI-19_ODP[01] elements>*** are removed from datasets;
	SI-19b.	the effectiveness of de-identification is evaluated ***<SI-19_ODP[02] frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-19-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; de-identification procedures; system configuration; datasets with personally identifiable information removed; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SI-19-Interview	[SELECT FROM: Organizational personnel responsible for identifying unnecessary identifiers; organizational personnel responsible for removing personally identifiable information from datasets; organizational personnel with information security and privacy responsibilities].
	SI-19-Test	[SELECT FROM: Automated mechanisms supporting and/or implementing the removal of personally identifiable information elements].

SI-19(01)	DE-IDENTIFICATION | COLLECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-19(01)	the dataset is de-identified upon collection by not collecting personally identifiable information.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-19(01)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; de-identification procedures; procedures for minimizing the collection of personally identifiable information; system configuration; data collection mechanisms; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SI-19(01)-Interview	[SELECT FROM: Organizational personnel responsible for de-identifying the dataset; organizational personnel with information security and privacy responsibilities].
	SI-19(01)-Test	[SELECT FROM: Automated mechanisms preventing the collection of personally identifiable information].

SI-19(02)	DE-IDENTIFICATION | ARCHIVING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-19(02)	the archiving of personally identifiable information elements is prohibited if those elements in a dataset will not be needed after the dataset is archived.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-19(02)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; de-identification procedures; system configuration documentation; data archiving mechanisms; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SI-19(02)-Interview	[SELECT FROM: Organizational personnel responsible for de-identifying the dataset; organizational personnel with dataset archival responsibilities; organizational personnel with information security and privacy responsibilities].
	SI-19(02)-Test	[SELECT FROM: Automated mechanisms prohibiting the archival of personally identifiable information elements].

SI-19(03)	DE-IDENTIFICATION | RELEASE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-19(03)	personally identifiable information elements are removed from a dataset prior to its release if those elements in the dataset do not need to be part of the data release.

SI-19(03)	DE-IDENTIFICATION | RELEASE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-19(03)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; de-identification procedures; procedures for minimizing the release of personally identifiable information; system configuration; data release mechanisms; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SI-19(03)-Interview	[SELECT FROM: Organizational personnel responsible for de-identifying the dataset; organizational personnel with information security and privacy responsibilities].
	SI-19(03)-Test	[SELECT FROM: Automated mechanisms supporting and/or implementing the removal of personally identifiable information elements from a dataset].

SI-19(04)	DE-IDENTIFICATION | REMOVAL, MASKING, ENCRYPTION, HASHING, OR REPLACEMENT OF DIRECT IDENTIFIERS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-19(04)	direct identifiers in a dataset are removed, masked, encrypted, hashed, or replaced.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-19(04)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; de-identification procedures; system configuration; documentation of de-identified datasets; tools for the removal, masking, encryption, hashing or replacement of direct identifiers; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SI-19(04)-Interview	[SELECT FROM: Organizational personnel responsible for de-identifying the dataset; organizational personnel with information security and privacy responsibilities].
	SI-19(04)-Test	[SELECT FROM: Automated mechanisms supporting and/or implementing the removal, masking, encryption, hashing or replacement of direct identifiers].

SI-19(05)	DE-IDENTIFICATION | STATISTICAL DISCLOSURE CONTROL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-19(05)[01]	numerical data is manipulated so that no individual or organization is identifiable in the results of the analysis;
	SI-19(05)[02]	contingency tables are manipulated so that no individual or organization is identifiable in the results of the analysis;
	SI-19(05)[03]	statistical findings are manipulated so that no individual or organization is identifiable in the results of the analysis.

SI-19(05)	DE-IDENTIFICATION | STATISTICAL DISCLOSURE CONTROL	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-19(05)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; de-identification procedures; system configuration; de-identified datasets; statistical analysis report; tools for the control of statistical disclosure; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SI-19(05)-Interview	[SELECT FROM: Organizational personnel responsible for de-identifying the dataset; organizational personnel with information security and privacy responsibilities].
	SI-19(05)-Test	[SELECT FROM: Automated mechanisms supporting and/or implementing the control of statistical disclosure].

SI-19(06)	DE-IDENTIFICATION | DIFFERENTIAL PRIVACY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-19(06)	the disclosure of personally identifiable information is prevented by adding non-deterministic noise to the results of mathematical operations before the results are reported.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-19(06)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; de-identification procedures; system configuration; de-identified datasets; differential privacy tools; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SI-19(06)-Interview	[SELECT FROM: Organizational personnel responsible for de-identifying the dataset; organizational personnel with information security and privacy responsibilities].
	SI-19(06)-Test	[SELECT FROM: Online query systems; automated mechanisms supporting and/or implementing differential privacy].

SI-19(07)	DE-IDENTIFICATION | VALIDATED ALGORITHMS AND SOFTWARE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-19(07)[01]	de-identification is performed using validated algorithms;
	SI-19(07)[02]	de-identification is performed using software that is validated to implement the algorithms.

SI-19(07)	DE-IDENTIFICATION | VALIDATED ALGORITHMS AND SOFTWARE	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-19(07)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; de-identification procedures; system configuration; de-identified datasets; algorithm and software validation tools; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SI-19(07)-Interview	[SELECT FROM: Organizational personnel responsible for de-identifying the dataset; organizational personnel with information security and privacy responsibilities].
	SI-19(07)-Test	[SELECT FROM: Validated algorithms and software].

SI-19(08)	DE-IDENTIFICATION | MOTIVATED INTRUDER	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-19(08)	a motivated intruder test is performed on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-19(08)-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; de-identification procedures; system configuration; motivated intruder test procedures; de-identified datasets; system security plan; privacy plan; privacy impact assessment; privacy risk assessment documentation; other relevant documents or records].
	SI-19(08)-Interview	[SELECT FROM: Organizational personnel responsible for de-identifying the dataset; organizational personnel with information security and privacy responsibilities].
	SI-19(08)-Test	[SELECT FROM: Motivated intruder test].

SI-20	TAINTING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-20_ODP	***the systems or system components with data or capabilities to be embedded are defined;***
	SI-20	data or capabilities are embedded in ***<SI-20_ODP systems or system components>*** to determine if organizational data has been exfiltrated or improperly removed from the organization.

SI-20	TAINTING	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-20-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; procedures addressing software and information integrity; system design documentation; system configuration settings and associated documentation; policy and procedures addressing the systems security engineering technique of deception; system security plan; privacy plan; other relevant documents or records].
	SI-20-Interview	[SELECT FROM: Organizational personnel responsible for detecting tainted data; organizational personnel with systems security engineering responsibilities; organizational personnel with information security and privacy responsibilities].
	SI-20-Test	[SELECT FROM: Automated mechanisms for post-breach detection; decoys, traps, lures, and methods for deceiving adversaries; detection and notification mechanisms].

SI-21	INFORMATION REFRESH	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-21_ODP[01]	***the information to be refreshed is defined;***
	SI-21_ODP[02]	***the frequencies at which to refresh information are defined;***
	SI-21	the ***<SI-21_ODP[01] information>*** is refreshed ***<SI-21_ODP[02] frequencies>*** or is generated on demand and deleted when no longer needed.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-21-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; procedures addressing software and information integrity; system design documentation; system configuration settings and associated documentation; information refresh procedures; list of information to be refreshed; system security plan; privacy plan; other relevant documents or records].
	SI-21-Interview	[SELECT FROM: Organizational personnel responsible for refreshing information; organizational personnel with information security and privacy responsibilities; organizational personnel with systems security engineering responsibilities; system developers].
	SI-21-Test	[SELECT FROM: Mechanisms for information refresh; organizational processes for information refresh].

SI-22	INFORMATION DIVERSITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-22_ODP[01]	***alternative information sources for essential functions and services are defined;***

SI-22	INFORMATION DIVERSITY	
	SI-22_ODP[02]	***essential functions and services that require alternative sources of information are defined;***
	SI-22_ODP[03]	***systems or system components that require an alternative information source for the execution of essential functions or services are defined;***
	SI-22a.	***<SI-22_ODP[01] alternative information sources>*** for ***<SI-22_ODP[02] essential functions and services>*** are identified;
	SI-22b.	an alternative information source is used for the execution of essential functions or services on ***<SI-22_ODP[03] systems or system components>*** when the primary source of information is corrupted or unavailable.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-22-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; system design documentation; system configuration settings and associated documentation; list of information sources; system security plan; privacy plan; other relevant documents or records].
	SI-22-Interview	[SELECT FROM: Organizational personnel with information security and privacy responsibilities; organizational personnel with systems security engineering responsibilities; system developers].
	SI-22-Test	[SELECT FROM: Automated methods and mechanisms to convert information from an analog to digital medium].

SI-23	INFORMATION FRAGMENTATION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SI-23_ODP[01]	***circumstances that require information fragmentation are defined;***
	SI-23_ODP[02]	***the information to be fragmented is defined;***
	SI-23_ODP[03]	***systems or system components across which the fragmented information is to be distributed are defined;***
	SI-23a.	under ***<SI-23_ODP[01] circumstances>***, ***<SI-23_ODP[02] information>*** is fragmented;
	SI-23b.	under ***<SI-23_ODP[01] circumstances>*** , the fragmented information is distributed across ***<SI-23_ODP[03] systems or system components>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SI-23-Examine	[SELECT FROM: System and information integrity policy; system and information integrity procedures; personally identifiable information processing policy; procedures addressing software and information integrity; system design documentation; system configuration settings and associated documentation; procedures to identify information for fragmentation and distribution across systems/system components; list of distributed and fragmented information; list of circumstances requiring information fragmentation; enterprise architecture; system security architecture; system security plan; privacy plan; other relevant documents or records].

SI-23	INFORMATION FRAGMENTATION	
	SI-23-Interview	[SELECT FROM: Organizational personnel with information security and privacy responsibilities; organizational personnel with systems security engineering responsibilities; system developers; security architects].
	SI-23-Test	[SELECT FROM: Organizational processes to identify information for fragmentation and distribution across systems/system components; automated mechanisms supporting and/or implementing information fragmentation and distribution across systems/system components].

4.20 SUPPLY CHAIN RISK MANAGEMENT

SR-01	POLICY AND PROCEDURES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-01_ODP[01]	***personnel or roles to whom supply chain risk management policy is to be disseminated to is/are defined;***
	SR-01_ODP[02]	***personnel or roles to whom supply chain risk management procedures are disseminated to is/are defined;***
	SR-01_ODP[03]	***one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};***
	SR-01_ODP[04]	***an official to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures is defined;***
	SR-01_ODP[05]	***the frequency at which the current supply chain risk management policy is reviewed and updated is defined;***
	SR-01_ODP[06]	***events that require the current supply chain risk management policy to be reviewed and updated are defined;***
	SR-01_ODP[07]	***the frequency at which the current supply chain risk management procedure is reviewed and updated is defined;***
	SR-01_ODP[08]	***events that require the supply chain risk management procedures to be reviewed and updated are defined;***
	SR-01a.[01]	a supply chain risk management policy is developed and documented;
	SR-01a.[02]	the supply chain risk management policy is disseminated to ***<SR-01_ODP[01] personnel or roles>***;
	SR-01a.[03]	supply chain risk management procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls are developed and documented;
	SR-01a.[04]	the supply chain risk management procedures are disseminated to ***<SR-01_ODP[02] personnel or roles>***.
	SR-01a.01(a)[01]	the ***<SR-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** supply chain risk management policy addresses purpose;
	SR-01a.01(a)[02]	the ***<SR-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** supply chain risk management policy addresses scope;
	SR-01a.01(a)[03]	***<SR-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** supply chain risk management policy addresses roles;
	SR-01a.01(a)[04]	the ***<SR-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** supply chain risk management policy addresses responsibilities;
	SR-01a.01(a)[05]	the ***<SR-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** supply chain risk management policy addresses management commitment;
	SR-01a.01(a)[06]	the ***<SR-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** supply chain risk management policy addresses coordination among organizational entities;

SR-01	POLICY AND PROCEDURES	
	SR-01a.01(a)[07]	the ***<SR-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** supply chain risk management policy addresses compliance.
	SR-01a.01(b)	the ***<SR-01_ODP[03] SELECTED PARAMETER VALUE(S)>*** supply chain risk management policy is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines;
	SR-01b.	the ***<SR-01_ODP[04] official>*** is designated to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures;
	SR-01c.01[01]	the current supply chain risk management policy is reviewed and updated ***<SR-01_ODP[05] frequency>***;
	SR-01c.01[02]	the current supply chain risk management policy is reviewed and updated following ***<SR-01_ODP[06] events>***;
	SR-01c.02[01]	the current supply chain risk management procedures are reviewed and updated ***<SR-01_ODP[07] frequency>***;
	SR-01c.02[02]	the current supply chain risk management procedures are reviewed and updated following ***<SR-01_ODP[08] events>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-01-Examine	[SELECT FROM: Supply chain risk management policy; supply chain risk management procedures; system security plan; privacy plan; other relevant documents or records].
	SR-01-Interview	[SELECT FROM: Organizational personnel with supply chain risk management responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with acquisition responsibilities; organizational personnel with enterprise risk management responsibilities].

SR-02	SUPPLY CHAIN RISK MANAGEMENT PLAN	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-02_ODP[01]	***systems, system components, or system services for which a supply chain risk management plan is developed are defined;***
	SR-02_ODP[02]	***the frequency at which to review and update the supply chain risk management plan is defined;***
	SR-02a.[01]	a plan for managing supply chain risks is developed;
	SR-02a.[02]	the supply chain risk management plan addresses risks associated with the research and development of ***<SR-02_ODP[01] systems, system components, or system services>***;
	SR-02a.[03]	the supply chain risk management plan addresses risks associated with the design of ***<SR-02_ODP[01] systems, system components, or system services>***;
	SR-02a.[04]	the supply chain risk management plan addresses risks associated with the manufacturing of ***<SR-02_ODP[01] systems, system components, or system services>***;

SR-02	SUPPLY CHAIN RISK MANAGEMENT PLAN	
	SR-02a.[05]	the supply chain risk management plan addresses risks associated with the acquisition of ***<SR-02_ODP[01] systems, system components, or system services>***;
	SR-02a.[06]	the supply chain risk management plan addresses risks associated with the delivery of ***<SR-02_ODP[01] systems, system components, or system services>***;
	SR-02a.[07]	the supply chain risk management plan addresses risks associated with the integration of ***<SR-02_ODP[01] systems, system components, or system services>***;
	SR-02a.[08]	the supply chain risk management plan addresses risks associated with the operation and maintenance of ***<SR-02_ODP[01] systems, system components, or system services>***;
	SR-02a.[09]	the supply chain risk management plan addresses risks associated with the disposal of ***<SR-02_ODP[01] systems, system components, or system services>***;
	SR-02b.	the supply chain risk management plan is reviewed and updated ***<SR-02_ODP[02] frequency>*** or as required to address threat, organizational, or environmental changes;
	SR-02c.[01]	the supply chain risk management plan is protected from unauthorized disclosure;
	SR-02c.[02]	the supply chain risk management plan is protected from unauthorized modification.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-02-Examine	[SELECT FROM: Supply chain risk management policy; supply chain risk management procedures; supply chain risk management plan; system and services acquisition policy; system and services acquisition procedures; procedures addressing supply chain protection; procedures for protecting the supply chain risk management plan from unauthorized disclosure and modification; system development life cycle procedures; procedures addressing the integration of information security and privacy requirements into the acquisition process; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; list of supply chain threats; list of safeguards to be taken against supply chain threats; system life cycle documentation; inter-organizational agreements and procedures; system security plan; privacy plan; privacy program plan; other relevant documents or records].
	SR-02-Interview	[SELECT FROM: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities].
	SR-02-Test	[SELECT FROM: Organizational processes for defining and documenting the system development life cycle (SDLC); organizational processes for identifying SDLC roles and responsibilities; organizational processes for integrating supply chain risk management into the SDLC; mechanisms supporting and/or implementing the SDLC].

SR-02(01)	SUPPLY CHAIN RISK MANAGEMENT PLAN | ESTABLISH SCRM TEAM	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-02(01)_ODP[01]	***the personnel, roles, and responsibilities of the supply chain risk management team are defined;***

SR-02(01)	SUPPLY CHAIN RISK MANAGEMENT PLAN | ESTABLISH SCRM TEAM	
	SR-02(01)_ODP[02]	***supply chain risk management activities are defined;***
	SR-02(01)	a supply chain risk management team consisting of ***<SR-02(01)_ODP[01] personnel, roles and responsibilities>*** is established to lead and support ***<SR-02(01)_ODP[02] supply chain risk management activities>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-02(01)-Examine	[SELECT FROM: Supply chain risk management policy; supply chain risk management procedures; supply chain risk management team charter documentation; supply chain risk management strategy; supply chain risk management implementation plan; procedures addressing supply chain protection; system security plan; privacy plan; other relevant documents or records].
	SR-02(01)-Interview	[SELECT FROM: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities; organizational personnel with enterprise risk management responsibilities; legal counsel; organizational personnel with business continuity responsibilities].

SR-03	SUPPLY CHAIN CONTROLS AND PROCESSES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-03_ODP[01]	***the system or system component requiring a process or processes to identify and address weaknesses or deficiencies is defined;***
	SR-03_ODP[02]	***supply chain personnel with whom to coordinate the process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes is/are defined;***
	SR-03_ODP[03]	***supply chain controls employed to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events are defined;***
	SR-03_ODP[04]	***one or more of the following PARAMETER VALUES is/are selected: {security and privacy plans; supply chain risk management plan; <SR-03_ODP[05] document>};***
	SR-03_ODP[05]	***the document identifying the selected and implemented supply chain processes and controls is defined (if selected);***
	SR-03a.[01]	a process or processes is/are established to identify and address weaknesses or deficiencies in the supply chain elements and processes of ***<SR-03_ODP[01] system or system component>***;
	SR-03a.[02]	the process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of ***<SR-03_ODP[01] system or system component>*** is/are coordinated with ***<SR-03_ODP[02] supply chain personnel>***;
	SR-03b.	***<SR-03_ODP[03] supply chain controls>*** are employed to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events;
	SR-03c.	the selected and implemented supply chain processes and controls are documented in ***<SR-03_ODP[04] SELECTED PARAMETER VALUE(S)>***.

SR-03	SUPPLY CHAIN CONTROLS AND PROCESSES	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-03-Examine	[SELECT FROM: Supply chain risk management policy; supply chain risk management procedures; supply chain risk management strategy; supply chain risk management plan; systems and critical system components inventory documentation; system and services acquisition policy; system and services acquisition procedures; procedures addressing the integration of information security and privacy requirements into the acquisition process; solicitation documentation; acquisition documentation (including purchase orders); service level agreements; acquisition contracts for systems or services; risk register documentation; system security plan; privacy plan; other relevant documents or records].
	SR-03-Interview	[SELECT FROM: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities].
	SR-03-Test	[SELECT FROM: Organizational processes for identifying and addressing supply chain element and process deficiencies].

SR-03(01)	SUPPLY CHAIN CONTROLS AND PROCESSES | DIVERSE SUPPLY BASE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-03(01)_ODP[01]	***system components with a diverse set of sources are defined;***
	SR-03(01)_ODP[02]	***services with a diverse set of sources are defined;***
	SR-03(01)[01]	a diverse set of sources is employed for ***<SR-03(01)_ODP[01] system components>***;
	SR-03(01)[02]	a diverse set of sources is employed for ***<SR-03(01)_ODP[02] services>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-03(01)-Examine	[SELECT FROM: Supply chain risk management policy and procedures; system and services acquisition policy; planning policy; procedures addressing supply chain protection; physical inventory of critical systems and system components; inventory of critical suppliers, service providers, developers, and contracts; inventory records of critical system components; list of security safeguards ensuring an adequate supply of critical system components; system security plan; other relevant documents or records].
	SR-03(01)-Interview	[SELECT FROM: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain protection responsibilities].
	SR-03(01)-Test	[SELECT FROM: Organizational processes for defining and employing security safeguards to ensure an adequate supply of critical system components; processes to identify critical suppliers; mechanisms supporting and/or implementing the security safeguards that ensure an adequate supply of critical system components].

SR-03(02)	SUPPLY CHAIN CONTROLS AND PROCESSES | LIMITATION OF HARM	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-03(02)_ODP	***controls to limit harm from potential supply chain adversaries are defined;***
	SR-03(02)	***<SR-03(02)_ODP controls>*** are employed to limit harm from potential adversaries identifying and targeting the organizational supply chain.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-03(02)-Examine	[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; configuration management policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements into the acquisition process; procedures addressing the baseline configuration of the system; configuration management plan; system design documentation; system architecture and associated configuration documentation; solicitation documentation; acquisition documentation; acquisition contracts for the system, system component, or system service; threat assessments; vulnerability assessments; list of security safeguards to be taken to protect the organizational supply chain against potential supply chain threats; system security plan; other relevant documents or records].
	SR-03(02)-Interview	[SELECT FROM: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities].
	SR-03(02)-Test	[SELECT FROM: Organizational processes for defining and employing safeguards to limit harm from adversaries of the organizational supply chain; mechanisms supporting and/or implementing the definition and employment of safeguards to protect the organizational supply chain].

SR-03(03)	SUPPLY CHAIN CONTROLS AND PROCESSES | SUB-TIER FLOW DOWN	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-03(03)	the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-03(03)-Examine	[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; procedures addressing supply chain protection; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; inter-organizational agreements and procedures; system security plan; other relevant documents or records].
	SR-03(03)-Interview	[SELECT FROM: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities].
	SR-03(03)-Test	[SELECT FROM: Organizational processes for establishing inter-organizational agreements and procedures with supply chain entities].

SR-04	PROVENANCE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-04_ODP	***systems, system components, and associated data that require valid provenance are defined;***
	SR-04[01]	valid provenance is documented for ***<SR-04_ODP systems, system components, and associated data>***;
	SR-04[02]	valid provenance is monitored for ***<SR-04_ODP systems, system components, and associated data>***;
	SR-04[03]	valid provenance is maintained for ***<SR-04_ODP systems, system components, and associated data>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-04-Examine	[SELECT FROM: Supply chain risk management policy; supply chain risk management procedures; supply chain risk management plan; documentation of critical systems, critical system components, and associated data; documentation showing the history of ownership, custody, and location of and changes to critical systems or critical system components; system architecture; inter-organizational agreements and procedures; contracts; system security plan; privacy plan; personally identifiable information processing policy; other relevant documents or records].
	SR-04-Interview	[SELECT FROM: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities].
	SR-04-Test	[SELECT FROM: Organizational processes for identifying the provenance of critical systems and critical system components; mechanisms used to document, monitor, or maintain provenance].

SR-04(01)	PROVENANCE | IDENTITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-04(01)_ODP	***supply chain elements, processes, and personnel associated with systems and critical system components that require unique identification are defined;***
	SR-04(01)[01]	unique identification of ***<SR-04(01)_ODP supply chain elements, processes, and personnel>*** is established;
	SR-04(01)[02]	unique identification of ***<SR-04(01)_ODP supply chain elements, processes, and personnel>*** is maintained.

SR-04(01)	PROVENANCE | IDENTITY	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-04(01)-Examine	[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements into the acquisition process; list of supply chain elements, processes, and actors (associated with the system, system component, or system service) requiring implementation of unique identification processes, procedures, tools, mechanisms, equipment, techniques, and/or configurations; system security plan; other relevant documents or records].
	SR-04(01)-Interview	[SELECT FROM: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain protection responsibilities; organizational personnel with responsibilities for establishing and retaining the unique identification of supply chain elements, processes, and actors].
	SR-04(01)-Test	[SELECT FROM: Organizational processes for defining, establishing, and retaining unique identification for supply chain elements, processes, and actors; mechanisms supporting and/or implementing the definition, establishment, and retention of unique identification for supply chain elements, processes, and actors].

SR-04(02)	PROVENANCE | TRACK AND TRACE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-04(02)_ODP	***systems and critical system components that require unique identification for tracking through the supply chain are defined;***
	SR-04(02)[01]	the unique identification of ***<SR-04(02)_ODP systems and critical system components>*** is established for tracking through the supply chain;
	SR-04(02)[02]	the unique identification of ***<SR-04(02)_ODP systems and critical system components>*** is maintained for tracking through the supply chain.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-04(02)-Examine	[SELECT FROM: Supply chain risk management policy and procedures; system and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements into the acquisition process; supply chain risk management plan; list of supply chain elements, processes, and actors (associated with the system, system component, or system service) requiring implementation of unique identification processes, procedures, tools, mechanisms, equipment, techniques, and/or configurations; system security plan; other relevant documents or records].
	SR-04(02)-Interview	[SELECT FROM: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain protection responsibilities; organizational personnel with responsibilities for establishing and retaining the unique identification of supply chain elements, processes, and actors].

SR-04(02)	PROVENANCE | TRACK AND TRACE	
	SR-04(02)-Test	[SELECT FROM: Organizational processes for defining, establishing, and retaining unique identification for supply chain elements, processes, and actors; mechanisms supporting and/or implementing the definition, establishment, and retention of unique identification for supply chain elements, processes, and actors].

SR-04(03)	PROVENANCE | VALIDATE AS GENUINE AND NOT ALTERED	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-04(03)_ODP[01]	***controls to validate that the system or system component received is genuine are defined;***
	SR-04(03)_ODP[02]	***controls to validate that the system or system component received has not been altered are defined;***
	SR-04(03)[01]	***<SR-04(03)_ODP[01] controls>*** are employed to validate that the system or system component received is genuine;
	SR-04(03)[02]	***<SR-04(03)_ODP[02] controls>*** are employed to validate that the system or system component received has not been altered.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-04(03)-Examine	[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; procedures addressing supply chain protection; procedures addressing the security design principle of trusted components used in the specification, design, development, implementation, and modification of the system; system design documentation; procedures addressing the integration of information security requirements into the acquisition process; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; evidentiary documentation (including applicable configurations) indicating that the system or system component is genuine and has not been altered; system security plan; other relevant documents or records].
	SR-04(03)-Interview	[SELECT FROM: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities].
	SR-04(03)-Test	[SELECT FROM: Organizational processes for defining and employing validation safeguards; mechanisms supporting and/or implementing the definition and employment of validation safeguards; mechanisms supporting the application of the security design principle of trusted components in system specification, design, development, implementation, and modification].

SR-04(04)	PROVENANCE | SUPPLY CHAIN INTEGRITY — PEDIGREE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-04(04)_ODP[01]	***controls employed to ensure that the integrity of the system and system component are defined;***

SR-04(04)	PROVENANCE | SUPPLY CHAIN INTEGRITY — PEDIGREE	
	SR-04(04)_ODP[02]	***an analysis method to be conducted to validate the internal composition and provenance of critical or mission-essential technologies, products, and services to ensure the integrity of the system and system component is defined;***
	SR-04(04)[01]	***<SR-04(04)_ODP[01] controls>*** are employed to ensure the integrity of the system and system components;
	SR-04(04)[02]	***<SR-04(04)_ODP[02] analysis method>*** is conducted to ensure the integrity of the system and system components.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-04(04)-Examine	[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; procedures addressing supply chain protection; bill of materials for critical systems or system components; acquisition documentation; software identification tags; manufacturer declarations of platform attributes (e.g., serial numbers, hardware component inventory) and measurements (e.g., firmware hashes) that are tightly bound to the hardware itself; system security plan; other relevant documents or records].
	SR-04(04)-Interview	[SELECT FROM: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities].
	SR-04(04)-Test	[SELECT FROM: Organizational processes for identifying pedigree information; organizational processes to determine and validate the integrity of the internal composition of critical systems and critical system components; mechanisms to determine and validate the integrity of the internal composition of critical systems and critical system components].

SR-05	ACQUISITION STRATEGIES, TOOLS, AND METHODS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-05_ODP	***acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks are defined;***
	SR-05[01]	***<SR-05_ODP strategies, tools, and methods>*** are employed to protect against supply chain risks;
	SR-05[02]	***<SR-05_ODP strategies, tools, and methods>*** are employed to identify supply chain risks;
	SR-05[03]	***<SR-05_ODP strategies, tools, and methods>*** are employed to mitigate supply chain risks.

SR-05	ACQUISITION STRATEGIES, TOOLS, AND METHODS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-05-Examine	[SELECT FROM: Supply chain risk management policy; supply chain risk management procedures; supply chain risk management plan; system and services acquisition policy; system and services acquisition procedures; procedures addressing supply chain protection; procedures addressing the integration of information security and privacy requirements into the acquisition process; solicitation documentation; acquisition documentation (including purchase orders); service level agreements; acquisition contracts for systems, system components, or services; documentation of training, education, and awareness programs for personnel regarding supply chain risk; system security plan; privacy plan; other relevant documents or records].
	SR-05-Interview	[SELECT FROM: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with supply chain risk management responsibilities].
	SR-05-Test	[SELECT FROM: Organizational processes for defining and employing tailored acquisition strategies, contract tools, and procurement methods; mechanisms supporting and/or implementing the definition and employment of tailored acquisition strategies, contract tools, and procurement methods].

SR-05(01)	ACQUISITION STRATEGIES, TOOLS, AND METHODS | ADEQUATE SUPPLY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-05(01)_ODP[01]	***controls to ensure an adequate supply of critical system components are defined;***
	SR-05(01)_ODP[02]	***critical system components of which an adequate supply is required are defined;***
	SR-05(01)	***<SR-05(01)_ODP[01] controls>*** are employed to ensure an adequate supply of ***<SR-05(01)_ODP[02] critical system components>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-05(01)-Examine	[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management strategy; supply chain risk management plan; contingency planning documents; inventory of critical systems and system components; determination of adequate supply; system and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements into the acquisition process; procedures addressing the integration of acquisition strategies, contract tools, and procurement methods into the acquisition process; solicitation documentation; acquisition documentation; service level agreements; acquisition contracts for systems or services; purchase orders/requisitions for the system, system component, or system service from suppliers; system security plan; other relevant documents or records].
	SR-05(01)-Interview	[SELECT FROM: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities].

SR-05(01)	ACQUISITION STRATEGIES, TOOLS, AND METHODS | ADEQUATE SUPPLY	
	SR-05(01)-Test	[SELECT FROM: Organizational processes for defining and employing tailored acquisition strategies, contract tools, and procurement methods; mechanisms supporting and/or implementing the definition and employment of tailored acquisition strategies, contract tools, and procurement methods].

SR-05(02)	ACQUISITION STRATEGIES, TOOLS, AND METHODS | ASSESSMENTS PRIOR TO SELECTION, ACCEPTANCE, MODIFICATION, OR UPDATE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-05(02)[01]	the system, system component, or system service is assessed prior to selection;
	SR-05(02)[02]	the system, system component, or system service is assessed prior to acceptance;
	SR-05(02)[03]	the system, system component, or system service is assessed prior to modification;
	SR-05(02)[04]	the system, system component, or system service is assessed prior to update.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-05(02)-Examine	[SELECT FROM: System security plan; system and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements into the acquisition process; security test and evaluation results; vulnerability assessment results; penetration testing results; organizational risk assessment results; system security plan; other relevant documents or records].
	SR-05(02)-Interview	[SELECT FROM: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain protection responsibilities].
	SR-05(02)-Test	[SELECT FROM: Organizational processes for conducting assessments prior to selection, acceptance, or update; mechanisms supporting and/or implementing the conducting of assessments prior to selection, acceptance, or update].

SR-06	SUPPLIER ASSESSMENTS AND REVIEWS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-06_ODP	***the frequency at which to assess and review the supply chain-related risks associated with suppliers or contractors and the systems, system components, or system services they provide is defined;***
	SR-06	the supply chain-related risks associated with suppliers or contractors and the systems, system components, or system services they provide are assessed and reviewed ***<SR-06_ODP frequency>***.

SR-06	SUPPLIER ASSESSMENTS AND REVIEWS	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-06-Examine	[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management strategy; supply chain risk management plan; system and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements into the acquisition process; records of supplier due diligence reviews; system security plan; other relevant documents or records].
	SR-06-Interview	[SELECT FROM: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain protection responsibilities].
	SR-06-Test	[SELECT FROM: Organizational processes for conducting supplier reviews; mechanisms supporting and/or implementing supplier reviews].

SR-06(01)	SUPPLIER ASSESSMENTS AND REVIEWS | TESTING AND ANALYSIS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-06(01)_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {organizational analysis; independent third-party analysis; organizational testing; independent third-party testing};***
	SR-06(01)_ODP[02]	***supply chain elements, processes, and actors to be analyzed and tested are defined;***
	SR-06(01)	***<SR-06(01)_ODP[01] SELECTED PARAMETER VALUE(S)>*** is/are employed on ***<SR-06(01)_ODP[02] supply chain elements, processes, and actors>*** associated with the system, system component, or system service.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-06(01)-Examine	[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; procedures addressing supply chain protection; evidence of organizational analysis, independent third-party analysis, organizational penetration testing, and/or independent third-party penetration testing; list of supply chain elements, processes, and actors (associated with the system, system component, or system service) subject to analysis and/or testing; system security plan; other relevant documents or records].
	SR-06(01)-Interview	[SELECT FROM: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities; organizational personnel with responsibilities for analyzing and/or testing supply chain elements, processes, and actors].
	SR-06(01)-Test	[SELECT FROM: Organizational processes for defining and employing methods of analysis/testing of supply chain elements, processes, and actors; mechanisms supporting and/or implementing the analysis/testing of supply chain elements, processes, and actors].

SR-07	SUPPLY CHAIN OPERATIONS SECURITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-07_ODP	***Operations Security (OPSEC) controls to protect supply chain-related information for the system, system component, or system service are defined;***
	SR-07	***<SR-07_ODP OPSEC controls>*** are employed to protect supply chain-related information for the system, system component, or system service.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-07-Examine	[SELECT FROM: Supply chain risk management plan; supply chain risk management procedures; system and services acquisition policy; system and services acquisition procedures; procedures addressing supply chain protection; list of OPSEC controls to be employed; solicitation documentation; acquisition documentation; acquisition contracts for the system, system component, or system service; records of all-source intelligence analyses; system security plan; privacy plan; other relevant documents or records].
	SR-07-Interview	[SELECT FROM: Organizational personnel with acquisition responsibilities; organizational personnel with information security and privacy responsibilities; organizational personnel with OPSEC responsibilities; organizational personnel with supply chain risk management responsibilities].
	SR-07-Test	[SELECT FROM: Organizational processes for defining and employing OPSEC safeguards; mechanisms supporting and/or implementing the definition and employment of OPSEC safeguards].

SR-08	NOTIFICATION AGREEMENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-08_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {notification of supply chain compromises; <SR-08_ODP[02] results of assessments or audits>};***
	SR-08_ODP[02]	***information for which agreements and procedures are to be established are defined (if selected);***
	SR-08	agreements and procedures are established with entities involved in the supply chain for the system, system components, or system service for ***<SR-08_ODP[01] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-08-Examine	[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; procedures addressing supply chain protection; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; inter-organizational agreements and procedures; system security plan; other relevant documents or records].
	SR-08-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities].

SR-08	NOTIFICATION AGREEMENTS	
	SR-08-Test	[SELECT FROM: Organizational processes for establishing inter-organizational agreements and procedures with supply chain entities].

SR-09	TAMPER RESISTANCE AND DETECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-09	a tamper protection program is implemented for the system, system component, or system service.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-09-Examine	[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; procedures addressing supply chain protection; procedures addressing tamper resistance and detection; tamper protection program documentation; tamper protection tools and techniques documentation; tamper resistance and detection tools and techniques documentation; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; system security plan; other relevant documents or records].
	SR-09-Interview	[SELECT FROM: Organizational personnel with tamper protection program responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities].
	SR-09-Test	[SELECT FROM: Organizational processes for the implementation of the tamper protection program; mechanisms supporting and/or implementing the tamper protection program].

SR-09(01)	TAMPER RESISTANCE AND DETECTION | MULTIPLE STAGES OF SYSTEM DEVELOPMENT LIFE CYCLE	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-09(01)	anti-tamper technologies, tools, and techniques are employed throughout the system development life cycle.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-09(01)-Examine	[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; procedures addressing tamper resistance and detection; tamper protection program documentation; tamper protection tools and techniques documentation; tamper resistance and detection tools (technologies) and techniques documentation; system development life cycle documentation; procedures addressing supply chain protection; system development life cycle procedures; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; inter-organizational agreements and procedures; system security plan; other relevant documents or records].

SR-09(01)	TAMPER RESISTANCE AND DETECTION | MULTIPLE STAGES OF SYSTEM DEVELOPMENT LIFE CYCLE	
	SR-09(01)-Interview	[SELECT FROM: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities; organizational personnel with SDLC responsibilities].
	SR-09(01)-Test	[SELECT FROM: Organizational processes for employing anti-tamper technologies; mechanisms supporting and/or implementing anti-tamper technologies].

SR-10	INSPECTION OF SYSTEMS OR COMPONENTS	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-10_ODP[01]	***systems or system components that require inspection are defined;***
	SR-10_ODP[02]	***one or more of the following PARAMETER VALUES is/are selected: {at random; at <SR-10_ODP[03] frequency>; upon <SR-10_ODP[04] indications of need for inspection>};***
	SR-10_ODP[03]	***frequency at which to inspect systems or system components is defined (if selected);***
	SR-10_ODP[04]	***indications of the need for an inspection of systems or system components are defined (if selected);***
	SR-10	***<SR-10_ODP[01] systems or system components>*** are inspected ***<SR-10_ODP[02] SELECTED PARAMETER VALUE(S)>*** to detect tampering.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-10-Examine	[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; records of random inspections; inspection reports/results; assessment reports/results; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; inter-organizational agreements and procedures; system security plan; other relevant documents or records].
	SR-10-Interview	[SELECT FROM: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities].
	SR-10-Test	[SELECT FROM: Organizational processes for establishing inter-organizational agreements and procedures with supply chain entities; organizational processes to inspect for tampering].

SR-11	COMPONENT AUTHENTICITY	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-11_ODP[01]	***one or more of the following PARAMETER VALUES is/are selected: {source of counterfeit component; <SR-11_ODP[02] external reporting organizations>; <SR-11_ODP[03] personnel or roles>};***

SR-11	COMPONENT AUTHENTICITY	
	SR-11_ODP[02]	***external reporting organizations to whom counterfeit system components are to be reported is/are defined (if selected);***
	SR-11_ODP[03]	***personnel or roles to whom counterfeit system components are to be reported is/are defined (if selected);***
	SR-11a.[01]	an anti-counterfeit policy is developed and implemented;
	SR-11a.[02]	anti-counterfeit procedures are developed and implemented;
	SR-11a.[03]	the anti-counterfeit procedures include the means to detect counterfeit components entering the system;
	SR-11a.[04]	the anti-counterfeit procedures include the means to prevent counterfeit components from entering the system;
	SR-11b.	counterfeit system components are reported to ***<SR-11_ODP[01] SELECTED PARAMETER VALUE(S)>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-11-Examine	[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; anti-counterfeit plan; anti-counterfeit policy and procedures; media disposal policy; media protection policy; incident response policy; reports notifying developers, manufacturers, vendors, contractors, and/or external reporting organizations of counterfeit system components; acquisition documentation; service level agreements; acquisition contracts for the system, system component, or system service; inter-organizational agreements and procedures; records of reported counterfeit system components; system security plan; other relevant documents or records].
	SR-11-Interview	[SELECT FROM: Organizational personnel with system and service acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities; organizational personnel with responsibilities for anti-counterfeit policies, procedures, and reporting].
	SR-11-Test	[SELECT FROM: Organizational processes for counterfeit prevention, detection, and reporting; mechanisms supporting and/or implementing anti-counterfeit detection, prevention, and reporting].

SR-11(01)	COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-11(01)_ODP	***personnel or roles requiring training to detect counterfeit system components (including hardware, software, and firmware) is/are defined;***
	SR-11(01)	***<SR-11(01)_ODP personnel or roles>*** are trained to detect counterfeit system components (including hardware, software, and firmware).

SR-11(01)	COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-11(01)-Examine	[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; system and services acquisition policy; anti-counterfeit plan; anti-counterfeit policy and procedures; media disposal policy; media protection policy; incident response policy; training materials addressing counterfeit system components; training records on the detection and prevention of counterfeit components entering the system; system security plan; other relevant documents or records].
	SR-11(01)-Interview	[SELECT FROM: Organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities; organizational personnel with responsibilities for anti-counterfeit policies, procedures, and training].
	SR-11(01)-Test	[SELECT FROM: Organizational processes for anti-counterfeit training].

SR-11(02)	COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-11(02)_ODP	***system components requiring configuration control are defined;***
	SR-11(02)[01]	configuration control over ***<SR-11(02)_ODP system components>*** awaiting service or repair is maintained;
	SR-11(02)[02]	configuration control over serviced or repaired ***<SR-11(02)_ODP system components>*** awaiting return to service is maintained.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-11(02)-Examine	[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; configuration control procedures; acquisition documentation; service level agreements; acquisition contracts for the system component; inter-organizational agreements and procedures; system security plan; other relevant documents or records].
	SR-11(02)-Interview	[SELECT FROM: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities].
	SR-11(02)-Test	[SELECT FROM: Organizational processes for establishing inter-organizational agreements and procedures with supply chain entities; organizational configuration control processes].

SR-11(03)	COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT SCANNING	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-11(03)_ODP	***the frequency at which to scan for counterfeit system components is defined;***

SR-11(03)	COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT SCANNING	
	SR-11(03)	scanning for counterfeit system components is conducted ***<SR-11(03)_ODP frequency>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-11(03)-Examine	[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; anti-counterfeit policy and procedures; system design documentation; system configuration settings and associated documentation; scanning tools and associated documentation; scanning results; procedures addressing supply chain protection; acquisition documentation; inter-organizational agreements and procedures; system security plan; other relevant documents or records].
	SR-11(03)-Interview	[SELECT FROM: Organizational personnel with system and services acquisition responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain risk management responsibilities; organizational personnel with responsibilities for anti-counterfeit policies and procedures; organizational personnel with responsibility for anti-counterfeit scanning].
	SR-11(03)-Test	[SELECT FROM: Organizational processes for scanning for counterfeit system components; mechanisms supporting and/or implementing anti-counterfeit scanning].

SR-12	COMPONENT DISPOSAL	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SR-12_ODP[01]	***data, documentation, tools, or system components to be disposed of are defined;***
	SR-12_ODP[02]	***techniques and methods for disposing of data, documentation, tools, or system components are defined;***
	SR-12	***<SR-12_ODP[01] data, documentation, tools, or system components>*** are disposed of using ***<SR-12_ODP[02] techniques and methods>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SR-12-Examine	[SELECT FROM: Supply chain risk management policy and procedures; supply chain risk management plan; disposal procedures addressing supply chain protection; media disposal policy; media protection policy; disposal records for system components; documentation of the system components identified for disposal; documentation of the disposal techniques and methods employed for system components; system security plan; other relevant documents or records].
	SR-12-Interview	[SELECT FROM: Organizational personnel with system component disposal responsibilities; organizational personnel with information security responsibilities; organizational personnel with supply chain protection responsibilities].
	SR-12-Test	[SELECT FROM: Organizational techniques and methods for system component disposal; mechanisms supporting and/or implementing system component disposal].

REFERENCES

LAWS, POLICIES, DIRECTIVES, REGULATIONS, STANDARDS, AND GUIDELINES[52]

LAWS AND EXECUTIVE ORDERS	
[EGOV]	E-Government Act [includes FISMA] (P.L. 107-347), December 2002. https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf
[FISMA]	Federal Information Security Modernization Act (P.L. 113-283), December 2014. https://www.govinfo.gov/app/details/PLAW-113publ283
[FOIA96]	Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996. https://www.govinfo.gov/content/pkg/PLAW-104publ231/pdf/PLAW-104publ231.pdf
[PRIVACT]	Privacy Act (P.L. 93-579), December 1974. https://www.govinfo.gov/content/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf
[USC 3502]	"Definitions," Title 44 U.S. Code, Sec. 3502. 2011 ed. https://www.govinfo.gov/app/details/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapI-sec3502
[USC 11101]	"Definitions," Title 40 U.S. Code, Sec. 11101. 2018 ed. https://www.govinfo.gov/app/details/USCODE-2018-title40/USCODE-2018-title40-subtitleIII-chap111-sec11101
POLICIES, DIRECTIVES, AND INSTRUCTIONS	
[OMB A-130]	Office of Management and Budget Memorandum Circular A-130, *Managing Information as a Strategic Resource*, July 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
[OMB M-17-12]	Office of Management and Budget Memorandum 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf
[CNSSI 1253]	Committee on National Security Systems Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, March 2014. https://www.cnss.gov/CNSS/issuances/Instructions.cfm
[CNSSI 4009]	Committee on National Security Systems Instruction No. 4009, *Committee on National Security Systems (CNSS) Glossary*, April 2015. https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[52] The references cited in this appendix are those external publications that directly support the FISMA and Privacy Projects at NIST. Additional NIST standards, guidelines, and interagency reports are also cited throughout this publication, including in the references section of the applicable control assessment procedures in Chapter Four. Direct links to the NIST website are provided to obtain access to those publications.

STANDARDS, GUIDELINES, AND REPORTS	
[FIPS 140-3]	National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3
[FIPS 199]	National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 199. https://doi.org/10.6028/NIST.FIPS.199
[FIPS 200]	National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) 200. https://doi.org/10.6028/NIST.FIPS.200
[ISO 15026]	International Organization for Standardization/International Electrotechnical Commission (2019) *ISO/IEC/IEEE 15026-1:2019 — Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary* https://www.iso.org/standard/73567.html
[ISO 15288]	International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers (2015) *ISO/IEC/IEEE 15288:2015 — Systems and software engineering — Systems life cycle processes*. https://www.iso.org/standard/63711.html
[ISO 15408]	International Organization for Standardization/International Electrotechnical Commission (2009) *ISO/IEC/IEEE 15408-1:2009 — Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
[ISO 29100]	International Organization for Standardization/International Electrotechnical Commission 29100:2011, Information technology—Security techniques—Privacy framework, December 2011. https://www.iso.org/standard/45123.html
[SP 800-18]	Swanson MA, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-18, Rev. 1. https://doi.org/10.6028/NIST.SP.800-18r1
[SP 800-30]	Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[SP 800-37] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[SP 800-39] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: Organization, Mission, and Information System View. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[SP 800-40] Souppaya MP, Scarfone KA (2013) Guide to Enterprise Patch Management Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 3. https://doi.org/10.6028/NIST.SP.800-40r3

[SP 800-47] Dempsey KL, Pillitteri VY, Regenscheid A (2021) Managing the Security of Information Exchanges. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-47, Rev. 1. https://doi.org/10.6028/NIST.SP.800-47r1

[SP 800-53] Joint Task Force Transformation Initiative (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of December 20, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[SP 800-53B] Joint Task Force (2020) Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B. https://doi.org/10.6028/NIST.SP.800-53B

[SP 800-60-1] Stine KM, Kissel RL, Barker WC, Fahlsing J, Gulick J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 1, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v1r1

[SP 800-60-2] Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J (2008) Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-60, Vol. 2, Rev. 1. https://doi.org/10.6028/NIST.SP.800-60v2r1

[SP 800-115] Scarfone KA, Souppaya MP, Cody A, Orebaugh AD (2008) Technical Guide to Information Security Testing and Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-115. https://doi.org/10.6028/NIST.SP.800-115

[SP 800-128] Johnson LA, Dempsey KL, Ross RS, Gupta S, Bailey D (2011) Guide for Security-Focused Configuration Management of Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-128, Includes updates as of October 10, 2019. https://doi.org/10.6028/NIST.SP.800-128

[SP 800-137] Dempsey KL, Chawla NS, Johnson LA, Johnston R, Jones AC, Orebaugh AD, Scholl MA, Stine KM (2011) Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137. https://doi.org/10.6028/NIST.SP.800-137

[SP 800-137A] Dempsey KL, Pillitteri VY, Baer C, Niemeyer R, Rudman R, Urban S (2020) Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-137A. https://doi.org/10.6028/NIST.SP.800-137A

[SP 800-161] Boyens JM, Paulsen C, Moorthy R, Bartol N (2015) Supply Chain Risk Management Practices for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161. https://doi.org/10.6028/NIST.SP.800-161

[SP 800-181] Petersen R, Santos D, Smith MC, Wetzel KA, Witte G (2020) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1

[IR 8011-1] Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 1: Overview. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 1. https://doi.org/10.6028/NIST.IR.8011-1

[IR 8011-2] Dempsey KL, Eavy P, Moore G (2017) Automation Support for Security Control Assessments: Volume 2: Hardware Asset Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 2. https://doi.org/10.6028/NIST.IR.8011-2

[IR 8011-3] Dempsey KL, Eavy P, Goren N, Moore G (2018) Automation Support for Security Control Assessments: Volume 3: Software Asset Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 3. https://doi.org/10.6028/NIST.IR.8011-3

[IR 8011-4]	Dempsey KL, Takamura E, Eavy P, Moore G (2020) Automation Support for Security Control Assessments: Volume 4: Software Vulnerability Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8011, Volume 4. https://doi.org/10.6028/NIST.IR.8011-4
[IR 8062]	Brooks S, Garcia M, Lefkovitz N, Lightman S, Nadeau E (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8062. https://doi.org/10.6028/NIST.IR.8062
WHITE PAPERS, WEBSITES, AND DATA SETS	
[FedRAMP]	General Services Administration (2022) *Federal Risk and Authorization Management Program (FedRAMP)*. https://www.fedramp.gov
[NARA CUI]	National Archives and Records Administration (2022) *Controlled Unclassified Information (CUI) Registry*. https://www.archives.gov/cui
[OSCAL]	National Institute of Standards and Technology (2022) *OSCAL: the Open Security Controls Assessment Language*. https://pages.nist.gov/OSCAL/
[OSCAL content]	National Institute of Standards and Technology (2022) *oscal-content* [usnistgov Git Repository]. https://github.com/usnistgov/oscal-content
[SEI]	Weinstock CB, Lipson HF, Goodenough J (2007) Arguing Security – Creating Security Assurance Cases. (Software Engineering Institute, Carnegie Mellon University, Pittsburg, PA.). https://resources.sei.cmu.edu/asset_files/WhitePaper/2013_019_001_293637.pdf

APPENDIX A

GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix A provides definitions for terminology used in NIST SP 800-53A. For other terminology in this publication, refer to the glossary in [SP 800-53], Revision 5. Sources for terms used in this publication are cited as applicable. Where no citation is noted, the source of the definition is Special Publication 800-53A.

activities	An assessment object that includes specific protection-related pursuits or actions supporting a system that involves people (e.g., conducting system backup operations, monitoring network traffic).
adequate security [OMB A-130]	Security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.
agency [OMB A-130]	Any executive agency or department, military department, Federal Government corporation, Federal Government-controlled corporation, or other establishment in the Executive Branch of the Federal Government, or any independent regulatory agency. See *executive agency*.
assessment	See *control assessment* or *risk assessment*.
assessment findings	Assessment results produced by the application of an assessment procedure to a security control, privacy control, or control enhancement to achieve an assessment objective; the execution of a determination statement within an assessment procedure by an assessor that results in either a satisfied or other than satisfied condition.
assessment method	One of three types of actions (i.e., examine, interview, test) taken by assessors in obtaining evidence during an assessment.
assessment object	The item (i.e., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment.

assessment objective	A set of determination statements that expresses the desired outcome for the assessment of a security control, privacy control, or control enhancement.
assessment plan	The objectives for the security and privacy control assessments and a detailed roadmap of how to conduct such assessments.
assessment procedure	A set of assessment objectives and an associated set of assessment methods and assessment objects.
assessment report	See *control assessment report.*
assessor	The individual, group, or organization responsible for conducting a security or privacy control assessment.
assignment operation	A control parameter that allows an organization to assign a specific, organization-defined value to the control or control enhancement (e.g., assigning a list of roles to be notified or a value for the frequency of testing). See *organization-defined parameters* and *selection operation*.
assurance [ISO 15026, Adapted]	Grounds for justified confidence that a [security or privacy] claim has been or will be achieved. *Note 1:* Assurance is typically obtained relative to a set of specific claims. The scope and focus of such claims may vary (e.g., security claims, safety claims) and the claims themselves may be interrelated. *Note 2:* Assurance is obtained through techniques and methods that generate credible evidence to substantiate claims.
assurance case [SEI]	A structured set of arguments and a body of evidence showing that a system satisfies specific claims with respect to a given quality attribute.
authorization [CNSSI 4009]	Access privileges granted to a user, program, or process or the act of granting those privileges.
authorization boundary [OMB A-130]	All components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected.
authorization to operate [OMB A-130]	The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.

authorizing official [OMB A-130]	A senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation.
availability [FISMA]	Ensuring timely and reliable access to and use of information.
baseline	See *control baseline*.
basic testing	A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object.
boundary [CNSSI 4009]	Physical or logical perimeter of a system. See also *authorization boundary* and *interface*.
breach [OMB M-17-12]	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for another than authorized purpose.
breadth	An attribute associated with an assessment method that addresses the scope or coverage of the assessment objects included with the assessment.
capability	A combination of mutually reinforcing security and/or privacy controls implemented by technical, physical, and procedural means. Such controls are typically selected to achieve a common information security- or privacy-related purpose.
chief information officer [OMB A-130]	The senior official that provides advice and other assistance to the head of the agency and other senior management personnel of the agency to ensure that IT is acquired and information resources are managed for the agency in a manner that achieves the agency's strategic goals and information resources management goals; and is responsible for ensuring agency compliance with, and prompt, efficient, and effective implementation of, the information policies and information resources management responsibilities, including the reduction of information collection burdens on the public.
chief information security officer	See *senior agency information security officer*.
chief privacy officer	See *senior agency official for privacy.*
common control [OMB A-130]	A security or privacy control that is inherited by multiple information systems or programs.

common control provider [SP 800-37]	An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security or privacy controls inheritable by systems).
compensating controls [SP 800-53B]	The security and privacy controls employed in lieu of the controls in the baselines described in NIST Special Publication 800-53B that provide equivalent or comparable protection for a system or organization.
component	See *system component*.
comprehensive testing	A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object.
confidentiality [FISMA]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
continuous monitoring [SP 800-137]	Maintaining ongoing awareness to support organizational risk decisions.
control	See *security control* or *privacy control*.
control assessment [SP 800-37]	The testing or evaluation of the controls in an information system or an organization to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security or privacy requirements for the system or the organization.
control assessment report [SP 800-37]	Documentation of the results of security and privacy control assessments, including information based on assessor findings and recommendations for correcting deficiencies in the implemented controls.
control assessor	See *assessor*.
control baseline [SP 800-53B]	Predefined sets of controls specifically assembled to address the protection needs of groups, organizations, or communities of interest. See *privacy control baseline* or *security control baseline*.
control effectiveness	A measure of whether a security or privacy control contributes to the reduction of information security or privacy risk.
control enhancement	Augmentation of a security or privacy control to build in additional but related functionality to the control, increase the strength of the control, or add assurance to the control.

control inheritance	A situation in which a system or application receives protection from security or privacy controls (or portions of controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See *common control*.
control parameter	See *organization-defined l parameter*.
countermeasures [FIPS 200]	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of a system. Synonymous with security controls and safeguards.
coverage	An attribute associated with an assessment method that addresses the scope or breadth of the assessment objects included in the assessment (e.g., types of objects to be assessed and the number of objects to be assessed by type). The values for the coverage attribute, hierarchically from less coverage to more coverage, are basic, focused, and comprehensive.
depth	An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method.
environment of operation [OMB A-130]	The physical surroundings in which an information system processes, stores, and transmits information.
examine	A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control or privacy control effectiveness over time.
executive agency [OMB A-130]	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.
federal agency	See *executive agency.*
federal information system [OMB A-130]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
focused testing	A test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object.

firmware [CNSSI 4009]	Computer programs and data stored in hardware – typically in read-only memory (ROM) or programmable read-only memory (PROM) – such that the programs and data cannot be dynamically written or modified during execution of the programs. See *hardware* and *software*.
hardware [CNSSI 4009]	The material physical components of a system. See *software* and *firmware*.
high-impact system [FIPS 200]	A system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of high.
hybrid control [OMB A-130]	A security or privacy control that is implemented for an information system in part as a common control and in part as a system-specific control.
individuals	An assessment object that includes people applying specifications, mechanisms, or activities.
impact	The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system.
impact value [FIPS 199]	The assessed worst-case potential impact that could result from a compromise of the confidentiality, integrity, or availability of information expressed as a value of low, moderate, or high.
information [OMB A-130]	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms.
information owner [SP 800-37]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
information resources [OMB A-130]	Information and related resources, such as personnel, equipment, funds, and information technology.
information security [OMB A-130]	The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
information security architecture [OMB A-130]	An embedded, integral part of the enterprise architecture that describes the structure and behavior of the enterprise security processes, security systems, personnel and organizational subunits, showing their alignment with the enterprise's mission and strategic plans.

information security policy [CNSSI 4009]	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
information security program plan [OMB A-130]	Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.
information security risk [SP 800-30]	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or systems.
information system [USC 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
information technology [USC 11101]	Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition, such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the life cycle of the equipment or service), and related resources. Information technology does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use.
information type [FIPS 199]	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
integrity [FISMA]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

interview	A type of assessment method that is characterized by the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control and privacy control effectiveness over time.
low-impact system [FIPS 200]	A system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS Publication 199 potential impact value of low.
mechanisms	An assessment object that includes specific protection-related items (e.g., hardware, software, or firmware).
moderate-impact system [FIPS 200]	A system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of moderate and no security objective is assigned a potential impact value of high.
national security system [OMB A-130]	Any system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
ongoing assessment	The continuous evaluation of the effectiveness of security control or privacy control implementation; with respect to security controls, a subset of Information Security Continuous Monitoring (ISCM) activities.
organization [FIPS 200, Adapted]	An entity of any size, complexity, or positioning within an organizational structure, including federal agencies, private enterprises, academic institutions, state, local, or tribal governments, or as appropriate, any of their operational elements.

organization-defined parameter	The variable part of a control or control enhancement that is instantiated by an organization during the tailoring process by either assigning an organization-defined value or selecting a value from a predefined list provided as part of the control or control enhancement. See *assignment operation* and *selection operation*.
parameter	See *organization-defined parameter*.
penetration testing	A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system.
personally identifiable information [OMB A-130]	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
personally identifiable information processing [ISO 29100, Adapted]	An operation or set of operations performed upon personally identifiable information that can include, but is not limited to, the collection, retention, logging, generation, transformation, use, disclosure, transfer, and disposal of personally identifiable information.
personally identifiable information processing permissions	The requirements for how personally identifiable information can be processed or the conditions under which personally identifiable information can be processed.
plan of action and milestones	A document that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, milestones for meeting the tasks, and the scheduled completion dates for the milestones.
potential impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (FIPS Publication 199 low); a serious adverse effect (FIPS Publication 199 moderate); or a severe or catastrophic adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.
privacy architecture [SP 800-37]	An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's privacy protection processes, technical measures, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.
privacy capability	See *capability.*
privacy control [OMB A-130]	The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks.

privacy control baseline	The set of privacy controls selected based on the privacy selection criteria that provide a starting point for the tailoring process.
privacy impact assessment [OMB A-130]	An analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis.
privacy plan [OMB A-130]	A formal document that details the privacy controls selected for an information system or environment of operation that are in place or planned for meeting applicable privacy requirements and managing privacy risks, details how the controls have been implemented, and describes the methodologies and metrics that will be used to assess the controls.
privacy program plan [OMB A-130]	A formal document that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the Senior Agency Official for Privacy and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.
privacy requirements	Requirements of an organization, information program, or system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission and business case needs with respect to privacy. Note: The term privacy requirement can be used in a variety of contexts from high-level policy activities to low-level implementation activities in system development and engineering disciplines.
reciprocity [SP 800-37]	Agreement among participating organizations to accept each other's security assessments to reuse system resources and/or to accept each other's assessed security posture to share information.

records [OMB A-130]	All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.
risk [OMB A-130]	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
risk assessment [SP 800-39]	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system.
[IR 8062, adapted]	Risk management includes threat and vulnerability analyses as well as analyses of adverse effects on individuals arising from information processing and considers mitigations provided by security and privacy controls planned or in place. Synonymous with *risk analysis*.
risk executive (function) [SP 800-37]	An individual or group within an organization that helps to ensure that security risk-related considerations for individual systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its mission and business functions; and managing risk from individual systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission or business success.
risk management [OMB A-130]	The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time.
risk mitigation [CNSSI 4009]	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.
risk response [OMB A-130]	Accepting, avoiding, mitigating, sharing, or transferring risk to agency operations, agency assets, individuals, other organizations, or the Nation.

risk tolerance [SP 800-39]	The level of risk or the degree of uncertainty that is acceptable to an organization.
scoping considerations	A part of tailoring guidance that provides organizations with specific considerations on the applicability and implementation of security and privacy controls in the control baselines. Considerations include policy or regulatory, technology, physical infrastructure, system component allocation, public access, scalability, common control, operational or environmental, and security objective.
security [CNSSI 4009]	A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach.
security capability	See *capability*.
security categorization	The process of determining the security category for information or a system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS Publication 199 for other than national security systems. See *security category*.
security category [OMB A-130]	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on agency operations, agency assets, individuals, other organizations, and the Nation.
security control [OMB A-130]	The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.
security control baseline [OMB A-130]	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.
security functionality	The security-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate.
security objective [FIPS 199]	Confidentiality, integrity, or availability.

security plan	A formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. The system security plan describes the system components that are included within the system, the environment in which the system operates, how the security requirements are implemented, and the relationships with or connections to other systems. See *system security plan*.
security requirement [FIPS 200, Adapted]	A requirement levied on an information system or an organization that is derived from applicable laws, executive orders, directives, regulations, policies, standards, procedures, or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted. *Note:* Security requirements can be used in a variety of contexts from high-level policy-related activities to low-level implementation-related activities in system development and engineering disciplines.
selection operation	A control parameter that allows an organization to select a value from a list of predefined values provided as part of the control or control enhancement (e.g., selecting to either restrict an action or prohibit an action). See *assignment operation* and *organization-defined parameter*.
senior agency information security officer	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. *Note:* Organizations subordinate to federal agencies may use the term *senior information security officer* or *chief information security officer* to denote individuals who fill positions with similar responsibilities to senior agency information security officers.
senior agency official for privacy [OMB A-130]	Senior official, designated by the head of each agency, who has agency-wide responsibility for privacy, including implementation of privacy protections; compliance with Federal laws, regulations, and policies relating to privacy; management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals.
senior information security officer	See *senior agency information security officer*.
software [CNSSI 4009]	Computer programs and associated data that may be dynamically written or modified during execution.

specification	An assessment object that includes document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, architectural designs) associated with a system.
subject	An individual, process, or device that causes information to flow among objects or change to the system state. Also see *object*.
supply chain	Linked set of resources and processes between and among multiple tiers of organizations, each of which is an acquirer, that begins with the sourcing of products and services and extends through their life cycle.
supply chain risk	The potential for harm or compromise that arises as a result of security risks from suppliers, their supply chains, and their products or services. Supply chain risks include exposures, threats, and vulnerabilities associated with the products and services traversing the supply chain as well as the exposures, threats, and vulnerabilities to the supply chain.
supply chain risk assessment	A systematic examination of supply chain risks, likelihoods of their occurrence, and potential impacts.
supply chain risk management	A systematic process for managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing risk response strategies to the risks presented by the supplier, the supplied products and services, or the supply chain.
system [CNSSI 4009]	Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. *Note:* Systems also include specialized systems such as industrial control systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.
[ISO 15288]	Combination of interacting elements organized to achieve one or more stated purposes. *Note 1:* There are many types of systems. Examples include: general and special-purpose information systems; command, control, and communication systems; crypto modules; central processing unit and graphics processor boards; industrial control systems; flight control systems; weapons, targeting, and fire control systems; medical devices and treatment systems; financial, banking, and merchandising transaction systems; and social networking systems. *Note 2:* The interacting elements in the definition of system include hardware, software, data, humans, processes, facilities, materials, and naturally occurring physical entities. *Note 3:* System-of-systems is included in the definition of system.
system component [SP 800-128]	A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware.

system owner (or program manager)	Official responsible for the overall procurement, development, integration, modification, operation, and maintenance of a system.
system security officer [SP 800-37]	Individual with assigned responsibility for maintaining the appropriate operational security posture for a system or program.
system security plan	See *security plan*.
system-related privacy risk [SP 800-37, Adapted]	Those risks that arise from the likelihood that a given operation the system is taking when processing PII could create an adverse effect on individuals—and the potential impact on individuals.
system-related security risk [SP 800-30]	Risk that arises through the loss of confidentiality, integrity, or availability of information or systems and that considers impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation. See *risk*.
system-specific control [OMB A-130]	A security or privacy control for an information system that is implemented at the system level and is not inherited by any other information system.
tailored control baseline	A set of controls that result from the application of tailoring guidance to a control baseline. See *tailoring*.
tailoring [SP 800-53B]	The process by which security control baselines are modified by: identifying and designating common controls, applying scoping considerations on the applicability and implementation of baseline controls, selecting compensating security controls, assigning specific values to organization-defined security control parameters, supplementing baselines with additional security controls or control enhancements, and providing additional specification information for control implementation.
tailoring assessment procedures	The process by which assessment procedures defined in SP 800-53A are adjusted or scoped to match the characteristics of a system under assessment, providing organizations with the flexibility needed to meet specific organizational requirements and avoid overly constrained assessment approaches.
test	A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control or privacy control effectiveness over time.
threat [SP 800-30]	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

threat assessment [CNSSI 4009]	Formal description and evaluation of threat to an information system.
threat source [FIPS 200]	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. See *threat agent*.
trustworthiness [CNSSI 4009]	The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.
trustworthiness (system)	The degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats. A trustworthy information system is believed to operate within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.
user	Individual, or (system) process acting on behalf of an individual, authorized to access a system. See *organizational user* and *non-organizational user*.
vulnerability [SP 800-30]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
vulnerability analysis	See *vulnerability assessment*.
vulnerability assessment [CNSSI 4009]	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

APPENDIX B

ACRONYMS

COMMON ABBREVIATIONS

CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CNSSI	Committee on National Security Systems Instruction
CONOPS	Concept of Operations
CUI	Controlled Unclassified Information
DNS	Domain Name System
DoD	Department of Defense
EMP	Electromagnetic pulse
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
I/O	Input/Output
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IR	Interagency Report or Internal Report
ISA	Interconnection Security Agreement
ISO	International Organization for Standardization
ISCM	Information Security Continuous Monitoring
IT	Information Technology
ITL	Information Technology Laboratory
MOU	Memorandum of Understanding
MTTF	Mean Time to Failure
NIAP	National Information Assurance Partnership

NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
ODP	Organization-Defined Parameter
OMB	Office of Management and Budget
OPSEC	Operation Security
OSCAL	Open Security Control Assessment Language
PDF	Portable Document Format
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification-Interoperable
PKI	Public Key Infrastructure
RMF	Risk Management Framework
SCRM	Supply Chain Risk Management
SDLC	System Development Life Cycle
SP	Special Publication
UTC	Coordinated Universal Time

APPENDIX C

ASSESSMENT METHOD DESCRIPTIONS

ASSESSMENT METHOD DEFINITIONS, APPLICABLE OBJECTS, AND ATTRIBUTES

This appendix defines the three assessment methods that can be used by assessors during security and privacy control assessments:

1. Examine
2. Interview
3. Test

Included in the definition of each assessment method are types of objects to which the method can be applied. The application of each method is described in terms of the attributes of depth and coverage, progressing from basic to focused to comprehensive. The attribute values correlate to the assurance requirements specified by the organization.

The depth attribute addresses the rigor and level of detail of the assessment. For the depth attribute, the focused attribute value includes and builds upon the assessment rigor and level of detail defined for the basic attribute value. The comprehensive attribute value includes and builds upon the assessment rigor and level of detail defined for the focused attribute value.

The coverage attribute addresses the scope or breadth of the assessment. For the coverage attribute, the focused attribute value includes and builds upon the number and type of assessment objects defined for the basic attribute value. The comprehensive attribute value includes and builds upon the number and type of assessment objects defined for the focused attribute value.

The use of bolded text in the assessment method description indicates content that was added and appears for the first time, signifying greater rigor and level of detail for the attribute value.

Assessment Method	Examine
Assessment Objects:	Specifications (e.g., policies, plans, procedures, system requirements, designs) Mechanisms (e.g., functionality implemented in hardware, software, firmware) Activities (e.g., system operations, administration, management, exercises)

Definition: The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security and privacy control existence, functionality, correctness, completeness, and potential for improvement over time.

Supplemental guidance: Typical assessor actions may include reviewing information security and privacy policies, plans, and procedures; analyzing system design documentation and interface specifications; observing system backup operations; reviewing the results of contingency plan exercises; observing incident response activities; studying technical manuals and user/administrator guides; checking, studying, or observing the operation of an information technology mechanism in the system hardware and software; or checking, studying, or observing physical security or privacy measures related to the operation of a system.

Attributes: Depth, Coverage

- The depth attribute addresses the rigor of and level of detail in the examination process. There are three possible values for the depth attribute: *basic*, *focused*, and *comprehensive.*

  Basic examination: Examination that consists of high-level reviews, checks, observations, or inspections of the assessment object. The basic examination is conducted using a limited body of evidence or documentation (e.g., functional-level descriptions for mechanisms; high-level process descriptions for activities; actual documents for specifications). Basic examinations provide a level of understanding of the security and privacy controls necessary for determining whether the controls are implemented and free of obvious errors.

  Focused examination: Examination that consists of high-level reviews, checks, observations, or inspections **and more in-depth studies/analyses** of the assessment object. The focused examination is conducted using a **substantial** body of evidence or documentation (e.g., functional-level descriptions **and, where appropriate and available, high-level design information** for mechanisms; high-level process descriptions **and implementation procedures** for activities; the actual documents **and related documents** for specifications). **Focused** examinations provide a level of understanding of the security and privacy controls necessary for determining whether the controls are implemented and free of obvious errors **and whether there are increased**

grounds for confidence that the controls are implemented correctly and operating as intended.

Comprehensive examination: Examination that consists of high-level reviews, checks, observations, or inspections and more in-depth, **detailed, and thorough** studies/analyses of the assessment object. The comprehensive examination is conducted using an **extensive** body of evidence or documentation (e.g., functional-level descriptions and, where appropriate and available, high-level design information, **low-level design information, and implementation information** for mechanisms; high-level process descriptions and **detailed** implementation procedures for activities; the actual documents and related documents for specifications[53]). **Comprehensive** examinations provide a level of understanding of the security and privacy controls necessary for determining whether the controls are implemented and free of obvious errors, there are **further** increased grounds for confidence that the controls are implemented correctly and operating as intended **on an ongoing and consistent basis, and there is support for continuous improvement in the effectiveness of the controls.**

- The *coverage* attribute addresses the scope or breadth of the examination process and includes the types of assessment objects to be examined, the number of objects to be examined (by type), and specific objects to be examined.[54] There are three possible values for the coverage attribute: *basic*, *focused*, and *comprehensive*.

  Basic examination: Examination that uses a representative sample of assessment objects (by type and number within type) to provide the level of coverage necessary for determining whether the security and privacy controls are implemented and free of obvious errors.

  Focused examination: Examination that uses a representative sample of assessment objects (by type and number within type) **and other specific assessment objects deemed particularly important to achieving the assessment objective** to provide the level of coverage necessary for determining whether the security and privacy controls are implemented and free of obvious errors **and whether there are increased grounds for confidence that the controls are implemented correctly and operating as intended.**

  Comprehensive examination: Examination that uses a **sufficiently large** sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide the level of coverage necessary for determining whether

[53] While additional documentation is likely needed for mechanisms when moving from basic to focused to comprehensive examinations, the documentation associated with specifications and activities may be the same or similar for focused and comprehensive examinations, with the rigor of the examinations of these documents being increased at the comprehensive level.

[54] The organization considers a variety of factors (e.g., available resources, importance of the assessment, the organization's overall assessment goals and objectives), confers with assessors, and provides direction on the type, number, and specific objects to be examined for the particular attribute value described.

the security and privacy controls are implemented and free of obvious errors, there are **further** increased grounds for confidence that the controls are implemented correctly and operating as intended **on an ongoing and consistent basis, and there is support for continuous improvement in the effectiveness of the controls.**

Assessment Method Interview

Assessment Objects: Individuals or groups of individuals

Definition: The process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security and privacy control existence, functionality, correctness, completeness, and potential for improvement over time.

Supplemental guidance: Typical assessor actions may include interviewing agency heads, chief information officers, senior agency information security officers, senior agency officials for privacy, authorizing officials, information owners, system and mission owners, system security and privacy officers, system security and privacy managers, personnel officers, human resource managers, legal, facilities managers, emergency management staff, training officers, system operators, network and system administrators, site managers, physical security officers, and users.

Attributes: Depth, Coverage

- The depth attribute addresses the rigor of and level of detail in the interview process. There are three possible values for the depth attribute: basic, focused, and comprehensive.

  Basic interview: Interview that consists of broad-based, high-level discussions with individuals or groups of individuals. The basic interview is conducted using a set of generalized, high-level questions. Basic interviews provide a level of understanding of the security and privacy controls necessary for determining whether the controls are implemented and free of obvious errors.

  Focused interview: Interview that consists of broad-based, high-level discussions **and more in-depth discussions in specific areas** with individuals or groups of individuals. The focused interview is conducted using a set of generalized, high-level questions **and more in-depth questions where the need for greater assurance or where responses indicate a need for more in-depth investigation. Focused** interviews provide a level of understanding of the security and privacy controls necessary for determining whether the controls are implemented and free of obvious errors **and whether there are increased grounds for confidence that the controls are implemented correctly and operating as intended.**

  Comprehensive interview**:** Interview that consists of broad-based, high-level discussions and **more in-depth, probing discussions in specific areas with individuals or groups of individuals**. The comprehensive interview is conducted using a set of generalized, high-level questions **and more in-depth, probing questions where the need for greater assurance or where responses indicate a need for more in-depth investigation. Comprehensive** interviews provide a level of understanding of the security and privacy controls necessary for determining whether the controls are implemented and free of obvious errors, there are **further** increased grounds for confidence that the controls are

implemented correctly and operating as intended **on an ongoing and consistent basis, and there is support for continuous improvement in the effectiveness of the controls.**

- The *coverage* attribute addresses the scope or breadth of the interview process and includes the types of individuals to be interviewed (by organizational role and associated responsibility), the number of individuals to be interviewed (by type), and specific individuals to be interviewed.[55] There are three possible values for the coverage attribute: *basic, focused, and comprehensive.*

  Basic interview: Interview that uses a representative sample of individuals in key organizational roles to provide the level of coverage necessary for determining whether the security and privacy controls are implemented and free of obvious errors.

  Focused interview**:** Interview that uses a representative sample of individuals in key organizational roles **and other specific individuals deemed particularly important to achieving the assessment objective** to provide the level of coverage necessary for determining whether the security and privacy controls are implemented and free of obvious errors **and whether there are increased grounds for confidence that the controls are implemented correctly and operating as intended.**

  Comprehensive interview: Interview that uses a **sufficiently large** sample of individuals in key organizational roles and other specific individuals deemed particularly important to achieving the assessment objective to provide the level of coverage necessary for determining whether the security and privacy controls are implemented and free of obvious errors, there are **further** increased grounds for confidence that the controls are implemented correctly and operating as intended **on an ongoing and consistent basis, and there is support for continuous improvement in the effectiveness of the controls.**

[55] The organization considers a variety of factors (e.g., available resources, importance of the assessment, the organization's overall assessment goals and objectives), confers with assessors, and provides direction on the type, number, and specific individuals to be interviewed for the particular attribute value described.

Assessment Method	Test
Assessment Objects:	Mechanisms (e.g., hardware, software, firmware) Activities (e.g., system operations, administration, management, exercises)

Definition: The process of exercising one or more assessment objects under specified conditions to compare actual with expected/desired behavior, the results of which are used to support the determination of security and privacy control existence, functionality, correctness, completeness, and potential for improvement over time.[56]

Supplemental guidance: Typical assessor actions may include testing access control, identification and authentication, and audit mechanisms; testing security and privacy configuration settings; testing physical access control devices; conducting penetration testing of key system components; testing system backup operations; testing the incident response capability; and exercising the contingency planning capability.

Attributes: Depth, Coverage

- The *depth* attribute addresses the types of testing to be conducted. There are three possible values for the depth attribute: *basic*, *focused*, and *comprehensive*.

  Basic testing: Test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Basic testing is conducted using a functional specification for mechanisms and a high-level process description for activities. Basic testing provides a level of understanding of the security and privacy controls necessary for determining whether the controls are implemented and free of obvious errors.

  Focused testing: Test methodology that assumes **some** knowledge of the internal structure and implementation detail of the assessment object. Focused testing is conducted using a functional specification **and limited system architectural information (e.g., high-level design)** for mechanisms and a high-level process description **and high-level description of integration into the operational environment** for activities. Focused testing provides a level of understanding of the security and privacy controls necessary for determining whether the controls are implemented and free of obvious errors **and whether there are increased grounds for confidence that the controls are implemented correctly and operating as intended.**

  Comprehensive testing: Test methodology that assumes **explicit and substantial** knowledge of the internal structure and implementation detail of the assessment object. Comprehensive testing is conducted using a functional

[56] Testing is typically used to determine if mechanisms or activities meet a set of predefined specifications. Testing can also be performed to determine characteristics of a security or privacy control that are not commonly associated with predefined specifications, such as penetration testing. Guidelines for conducting penetration testing are provided in Appendix D.

specification, **extensive** system architectural information (e.g., high-level design, **low-level design**), **implementation representation (e.g., source code, schematics)** for mechanisms, and a high-level process description and **detailed** description of integration into the operational environment for activities. Comprehensive testing provides a level of understanding of the security and privacy controls necessary for determining whether the controls are implemented and free of obvious errors, there are **further** increased grounds for confidence that the controls are implemented correctly and operating as intended **on an ongoing and consistent basis, and there is support for continuous improvement in the effectiveness of the controls.**

- The coverage attribute addresses the scope or breadth of the testing process and includes the types of assessment objects to be tested, the number of objects to be tested (by type), and specific objects to be tested.[57] There are three possible values for the coverage attribute: *basic*, *focused*, and *comprehensive*.

  Basic testing: Testing that uses a representative sample of assessment objects (by type and number within type) to provide the level of coverage necessary for determining whether the security and privacy controls are implemented and free of obvious errors.

  Focused testing: Testing that uses a representative sample of assessment objects (by type and number within type) **and other specific assessment objects deemed particularly important to achieving the assessment objective** to provide the level of coverage necessary for determining whether the security and privacy controls are implemented and free of obvious errors **and whether there are increased grounds for confidence that the controls are implemented correctly and operating as intended.**

  Comprehensive testing: Testing that uses a **sufficiently large** sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide the level of coverage necessary for determining whether the security and privacy controls are implemented and free of obvious errors, there are **further** increased grounds for confidence that the controls are implemented correctly and operating as intended **on an ongoing and consistent basis, and there is support for continuous improvement in the effectiveness of the controls.**

[57] The organization considers a variety of factors (e.g., available resources, importance of the assessment, the organization's overall assessment goals and objectives), confers with assessors, and provides direction on the type, number, and specific objects to be tested for the particular attribute value described. For mechanism-related testing, the coverage attribute also addresses the extent of the testing conducted (e.g., for software, the number of test cases and modules tested; for hardware, the range of inputs, number of components tested, and range of environmental factors over which the testing is conducted).

APPENDIX D

PENETRATION TESTING

ASSESSMENT TOOLS AND TECHNIQUES TO IDENTIFY SYSTEM WEAKNESSES

Organizations may consider adding controlled penetration testing to their arsenal of tools and techniques used to assess the security and privacy controls in organizational systems. Penetration testing is a specific type of assessment in which assessors simulate the actions of a given class of attacker by using a defined set of documentation (i.e., documentation representative of what that class of attacker is likely to possess) and working under other specific constraints to attempt to circumvent the security or privacy features of a system.

Penetration testing is conducted as a controlled attempt to breach the security and privacy controls employed within the system using the attacker's techniques and appropriate hardware and software tools. Penetration testing represents the results of a specific assessor or group of assessors at a specific point in time using agreed-upon *rules of engagement*. Considering the complexity of the information technologies commonly employed by organizations today, penetration testing can be viewed not as a means to verify the security and privacy features of a system but rather as a means to enhance the organization's understanding of the system, uncover weaknesses or deficiencies in the system, and indicate the level of effort required on the part of adversaries to breach the system's safeguards.

Penetration testing exercises can be scheduled and/or random in accordance with organizational policy and organizational assessments of risk. Consideration can be given to performing penetration tests on any newly developed system (or legacy system undergoing a major upgrade) before the system is authorized for operation, after important changes are made to the environment in which the system operates, and when a new type of attack is discovered that may impact the system. Organizations actively monitor the system environment and threat landscape (e.g., new vulnerabilities, attack techniques, new technology deployments, user security, and privacy awareness and training) to identify changes that require out-of-cycle penetration testing.

Organizations specify which components within the system are subject to penetration testing as well as the attacker's profile to be adopted throughout the penetration testing exercises. Organizations train selected personnel in the use and maintenance of penetration testing tools and techniques. Effective penetration testing tools have the capability to readily update the list of attack techniques and exploitable vulnerabilities used during the exercises. Organizations update the list of attack techniques and exploitable vulnerabilities used in penetration testing based on an organizational assessment of risk or when significant new vulnerabilities or threats are identified and reported. Whenever possible, organizations employ tools and attack techniques that include the capability to perform penetration testing exercises on systems and security and privacy controls in an automated manner.[58]

[58] While automated penetration testing tools provide repeatable results and reduce the resources used, organizations should carefully consider the potential detrimental effects of automated exploits on system availability. Additionally, penetration testing based solely on automated tools may not provide the level of attempted system compromise that organizations might experience from an actual attacker.

The information obtained from the penetration testing process can be shared with appropriate personnel throughout the organization to help prioritize the vulnerabilities in the system that are demonstrably subject to compromise by attackers of a profile equivalent to the ones used in the penetration testing exercises. The prioritization helps to determine effective strategies for eliminating the identified vulnerabilities and mitigating associated risks to the organization's operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of the system. Penetration testing can be integrated into the network security testing process and the patch and vulnerability management process.[59]

Penetration Testing Considerations

Organizations consider the following criteria when developing and implementing a controlled penetration testing program. An effective penetration test:

- Goes beyond vulnerability scanning to provide explicit proof of mission risks and an indicator of the level of effort that an adversary would need to expend in order to cause harm to the organization's operations and assets, individuals, other organizations, or the Nation
- Approaches the system as the adversary would – considering vulnerabilities, incorrect system configurations, trust relationships between organizations, and architectural weaknesses in the environment being tested
- Has a clearly defined scope and contains as a minimum:
    - A definition of the environment subject to testing (e.g., facilities, users, organizational groups)
    - A definition of the attack surface to be tested (e.g., servers, desktop systems, wireless networks, web applications, intrusion detection and prevention systems, firewalls, email accounts, user security and privacy awareness and training posture, and incident response posture, including breaches of personally identifiable information)
    - A definition of the threat sources to simulate (e.g., an enumeration of attackers' profiles to be used, such as an internal attacker, casual attacker, single or group of external targeted attackers, nation/state actor, or criminal organization)
    - A definition of the objectives for the simulated attacker (e.g., gain domain administrator access on the organization's LDAP [Lightweight Directory Access Protocol] structure and access and modify information in the organization's financial system)
    - A definition of level of effort (e.g., time and resources) to be expended

[59] [SP 800-40] provides guidance on patch and vulnerability management. [SP 800-115] provides guidance on information and network security testing.

  - A definition of the rules of engagement

- Thoroughly documents all activities performed during the test, including all exploited vulnerabilities and how the vulnerabilities were combined into attacks

- Produces results indicating a likelihood of occurrence for a given attack by using the level of effort that the team needed to expend to penetrate the system as an indicator of the penetration resistance of the system

- Validates existing security and privacy controls (including risk mitigation mechanisms, such as firewalls and intrusion detection and prevention systems)

- Provides a verifiable and reproducible log of all the activities performed during the test

- Provides actionable results with information about possible remediation measures for the successful attacks performed.

APPENDIX E

ASSESSMENT REPORTS

DOCUMENTING THE FINDINGS FROM SECURITY AND PRIVACY CONTROL ASSESSMENTS

The primary purpose of the *security* and *privacy assessment reports* is to convey the results of the security and privacy control assessments to appropriate organizational officials. The security assessment report and privacy assessment report are included in the system authorization package along with the system security plan and privacy plan (or equivalent for common controls), plan of action and milestones, and an executive summary to provide authorizing officials with the information necessary to make risk-based decisions on whether to authorize a system to begin operating or continue its operation. As the assessment and authorization process becomes more dynamic in nature, relying to a greater degree on the continuous monitoring aspects of the process as an integrated and tightly coupled part of the system development life cycle, the ability to update the security and privacy assessment reports frequently becomes a critical aspect of information security and privacy programs.

It is important to emphasize the relationship among the key artifacts in the authorization package, as described in [SP 800-37]. Artifacts in the authorization package provide a reliable indication of the overall security and privacy risk posture of the system and the ability of the system to protect the organization's operations and assets, individuals, other organizations, and the Nation to the degree necessary. The key artifacts are updated on an ongoing basis in accordance with the continuous monitoring program established by the organization.

The security and privacy assessment reports provide a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any weaknesses or deficiencies in the security and privacy controls.[60] This appendix provides a template for reporting the results from security and privacy control assessments. Organizations are not restricted to the specific template format. However, it is expected that the overall report of an assessment includes information similar to that detailed in the template for each security and privacy control assessed preceded by a summary that provides the list of all security and privacy controls assessed and the overall status of each control.

Key Elements for Assessment Reporting

The following elements are included in security and privacy assessment reports:[61]

- System name
- Security categorization
- Site(s) assessed and assessment date(s)
- Assessor's name/identification
- Previous assessment results (if reused)

[60] While the rationale for each determination made is a part of the formal security and privacy assessment reports, the complete set of records produced as part of the assessment is likely not included in the report. However, organizations retain the portion of the records necessary for maintaining an audit trail of assessment evidence, facilitating reuse of evidence, and promoting repeatability of assessor actions.

[61] Information available in other key organizational documents (e.g., security or privacy plans, risk assessments, plans of action and milestones, or security or privacy assessment plans) need not be duplicated in the security and privacy assessment reports.

- Security/privacy control or control enhancement designator
- Selected assessment methods and objects
- Depth and coverage attributes values
- Assessment finding summary (indicating “satisfied” or “other than satisfied”)
- Assessor comments (weaknesses or deficiencies noted)
- Assessor recommendations (priorities, remediation, corrective actions, or improvements)

The Assessment Findings

Each determination statement executed by an assessor results in one of the following findings: satisfied (S) or other than satisfied (O). Figure 9 provides an example of an assessment finding for CP-03.

During an actual security and privacy control assessment, the assessment findings, comments, and recommendations are documented using appropriate organization-defined reporting forms or platforms. Organizations are encouraged to develop standard templates for reporting that contain the key elements for assessment reporting described above. Whenever possible, automation is used to make assessment data collection and reporting cost-effective, timely, and efficient.

CP-03	CONTINGENCY TRAINING			
	ASSESSMENT OBJECTIVE *Determine if:*		**ASSESSMENT FINDING**	**ASSESSOR COMMENTS AND RECOMMENDATIONS**
	CP-03_ODP[01]	***the time period within which to provide contingency training after assuming a contingency role or responsibility is defined;***	S	System ABC contingency planning policy identifies (organization-defined) time period as 4 weeks.
	CP-03_ODP[02]	***frequency at which to provide training to system users with a contingency role or responsibility is defined;***	S	System ABC contingency planning policy identifies frequency as annually.
	CP-03_ODP[03]	***frequency at which to review and update contingency training content is defined;***	S	System ABC contingency planning policy identifies frequency as annually.
	CP-03_ODP[04]	***events necessitating review and update of contingency training are defined;***	O	No assessment artifacts identify events necessitating review and update of contingency training.
	CP-03a.01	*contingency training is provided to system users consistent with assigned roles and responsibilities within <CP -03_ODP[01] time period> of assuming a contingency role or responsibility;*	S	
	CP-03a.02	*contingency training is provided to system users consistent with assigned roles and responsibilities when required by system changes;*	O	Marked as "other than satisfied." Assessors could not find evidence that contingency training to system ABC users was provided consistent with their assigned roles and responsibilities when there were significant changes to the system.
	CP-03a.03	*contingency training is provided to system users consistent with assigned roles and responsibilities <CP -03_ODP[02] frequency> thereafter;*	S	
	CP-03b.[01]	*the contingency plan training content is reviewed and updated <CP-03_ODP[03] frequency>;*	S	
	CP-03b.[02]	*the contingency plan training content is reviewed and updated following <CP -03_ODP[04] events>.*	O	CP-03_ODP[04] is not defined; this objective cannot be assessed.

FIGURE 9: SECURITY AND PRIVACY CONTROL ASSESSMENT FINDINGS EXAMPLE

APPENDIX F

ONGOING ASSESSMENT AND AUTOMATION

USING AUTOMATED TECHNIQUES TO ACHIEVE MORE EFFICIENT ASSESSMENTS

Ongoing security and privacy assessment is the continuous evaluation of the effectiveness of security and privacy control implementation. Ongoing assessment is an essential subset of *Information Security Continuous Monitoring (ISCM)* activities.[62] Ongoing assessment encompasses ISCM Steps 3 and 4 and is initiated as part of ISCM Step 3, *Implement*, when the collection of security-related information begins in accordance with organization-defined frequencies. Ongoing assessment continues as the security-related information generated as part of ISCM Step 3 is correlated, analyzed, and reported to senior leaders as part of ISCM Step 4. As noted in [SP 800-137], security-related information is generated, correlated, analyzed, and reported using automated tools to the extent that it is possible and practical to do so. When it is not possible and practical to use automated tools, security-related information is generated, correlated, analyzed, and reported using manual or procedural methods. In this way, senior leaders are provided with the security-related information necessary to make credible, risk-based decisions regarding information security risk to the mission and business.[63]

Automating assessments is a fundamental element in helping organizations manage information security and privacy risks. Evolving threats and changes in PII processing create a challenge for organizations that design, implement, and operate complex systems compromised of many hardware, firmware, and software components. The ability to assess all implemented security and privacy controls as frequently as needed using manual or procedural methods has become impractical for most organizations due to the size, complexity, and scope of their information technology infrastructures.

One strategy to increase the number of security and privacy controls for which assessment and monitoring can be automated depends on defining a *desired state specification* and expressing the desired state in a form that can be compared automatically (i.e., in data) with the actual state. The desired state is a defined value or *specification* to which the actual state value can be compared. A mismatch of the two values indicates that a defect is present in the effectiveness of one or more controls. For example, an organizational policy may state that user accounts will be locked after three unsuccessful logon attempts. The desired state specification would be that applicable devices are configured to lock accounts after three unsuccessful logon attempts. If, during automated assessment, the security-related information collected indicates that a specific device is configured such that accounts are locked only after *five* unsuccessful logon attempts, a mismatch between the desired state (three attempts allowed before lockout) and the actual state (five attempts allowed before lockout) is identified. The mismatch may reflect a problem with the effectiveness of SP 800-53 control AC-7, Unsuccessful Logon Attempts; AC-2, Account Management; and/or CM-2, Baseline Configuration. When a desired state specification

[62] [SP 800-137] provides guidance on Information Security Continuous Monitoring (ISCM). [SP 800-137A] provides guidance on conducting assessments of ISCM Programs.

[63] Continuous monitoring can be effectively applied to privacy controls consistent with the concepts, techniques, and principles described in [SP 800-137]. Senior Agency Officials for Privacy (SAOPs)/Chief Privacy Officers (CPOs) provide guidance on the ongoing monitoring of privacy controls.

strategy is employed, security-related information generated from ISCM activities is equivalent to security control assessment results.

In order to effectively automate security and privacy control assessments using the desired state specification strategy, it is important to meet the following prerequisites:

- Automated actual state and behavior specifications are defined;
- Data-based desired state specifications (comparable to the actual state) are defined; and
- A method to compute or identify defects (i.e., differences between desired and actual state and behavior) is defined.

When the prerequisites are met, the assessment system can automatically compute where differences between the desired state and actual state (defects) occur, use that information to create security and privacy assessment reports, and deliver those reports to designated personnel via a security and privacy management console (dashboard).

When automated tools are used to conduct assessments, the test assessment method is used.[64] The organization determines and documents the specific capabilities[65] and privacy controls that are being assessed by the automated tool, the frequency with which the tool will assess the capabilities or controls, and the analysis and reporting requirements for the capabilities or controls.

To help automate ongoing assessment, NIST and the Department of Homeland Security Cybersecurity Infrastructure Security Agency (CISA) collaborated on the development of a process that leverages the *test* assessment method and is consistent with the Risk Management Framework, as described in SP 800-37 and the ISCM guidance in SP 800-137. The automation process is described in NIST Interagency/Internal Report (NISTIR) 8011, *Automation Support for Security Control Assessments: Volume 1: Overview* [IR 8011-1] which defines specific security capabilities and describes the overall automated assessment process. Specific methods to automate the assessment of each defined security capability is provided in subsequent NISTIR 8011 volumes. Automation of the test method for security assessments is facilitated by the CISA Continuous Diagnostics and Mitigation (CDM) program.

[64] If greater depth and coverage are needed to provide additional assurance, the automated test method may be supplemented by the use of manual or procedural assessment methods (i.e., interview, examine, or manual test).

[65] If a security or privacy capability is defined, a mapping of all individual controls that support the capability is documented. If organizations define multiple capabilities, a many-to-many relationship between security and privacy controls and capabilities is to be expected. See Section 3.5 for additional information regarding security and privacy capability assessments.