Information System Security Officer (ISSO) Guide

Office of the Chief Information Security Officer

Version 10

September 16, 2013

DEPARTMENT OF HOMELAND SECURITY

Document Change History

Version	Date	Description
0.1	11/25/09	Initial Internal Draft
0.2	12/15/09	Revised Internal Draft, corrected formatting and grammatical errors
0.3	1/27/2010	Incorporated ISO comments
1.0	3/30/2010	Final Version
8.0	6/06/2011	• Updated entire document for terminology changes per DHS 4300A Version 8.0 and NIST SP 800-37 • Changed version to match DHS 4300A • Created new section 2.1.2 Critical Control Review (CCR) Team • Updates: o 2.1.1 Document Review (DR) Team; o 2.1.4 DHS InfoSec Customer Service Center; • Appendix C: OIG Potential Listing of Security Test Tools & Utilities.
8.0	9/19/2011	• Section 5.1 ISSO letter Attachement N was changed to Attachement C.
10		• Document updated to reflect new IACS tool, Ongoing Authorization, and other minor changes. • ISO changed to DHS OCISO.

TABLE OF CONTENTS

LIST OF FIGURES

1.0 INTRODUCTION

1.1 Background

The Information System Security Officer (ISSO) serves as the principal advisor to the Information System Owner (SO), Business Process Owner, and the Chief Information Security Officer (CISO) / Information System Security Manager (ISSM) on all matters, technical and otherwise, involving the security of an information system. ISSOs are responsible for ensuring the implementation and maintenance of security controls in accordance with the Security Plan (SP) and Department of Homeland Security (DHS) policies. In almost all cases, ISSOs will be called on to provide guidance, oversight, and expertise, but they may or may not develop security documents or actually implement any security controls. While ISSOs will not actually perform all functions, they will have to coordinate, facilitate, or otherwise ensure certain activities are being performed. As a result, it is important for ISSOs to build relationships with the SO, technical staff, and other stakeholders as described in this document.

This guide provides basic information to help ISSOs fulfill their many responsibilities and serves as a foundation for Components to develop and implement their own ISSO guidance. It also provides techniques, procedures, and useful tips for implementing the requirements of the DHS Information Security Program for Sensitive Systems.

This guide is a compilation of the best practices used by DHS Components and requirements contained in various DHS policies and procedures, National Institute of Standards and Technology (NIST) publications, Office of Management and Budget (OMB) guidance and Congressional and Executive Orders.

1.2 Purpose

ISSO duties, responsibilities, functions, tasks, and chain of command vary widely, even within the same Component. The document provides practical guidance to assist DHS ISSOs when performing assigned tasks. It addresses and explains the responsibilities, duties, tasks, resources, and organizational relationships needed for an ISSO to be successful. ISSOs should use this document as a guide as it applies to their circumstances.

This document is meant to be a companion document to, and an elaboration of, the various DHS Management Directives (MDs), Information Technology (IT) Security Policies and Handbooks (e.g., DHS 4300A), as well as the procedures and tools to implement those policies.

1.3 Scope

The ISSO Guide provides practical guidance based on DHS directives and policies applicable throughout the Department. Many Components have additional guidance that tailors DHS guidance to meet specific Component requirements. In all cases, Component guidance should be used as the primary reference source as long as it is consistent with DHS directives and policies.

The information in this guide is intended to support ISSO responsibilities for Sensitive But Unclassified (SBU) systems. Although much of the information in this guide is applicable to

ISSOs for Classified systems, it cannot be considered authoritative for information systems processing National Security Information, Sensitive Compartmented Information (SCI), Cryptographic/Cryptologic data, or Special Access Programs. ISSOs for those excluded systems are guided by separate documentation including but not limited to the:

- DHS 4300B National Security System Policy
- DHS 4300B National Security Systems Handbook
- DHS 4300C Sensitive Compartmented Information (SCI) Systems Policy Directive
- DHS SCI Systems Information Assurance Handbook

1.4 DHS Information Security Program

The DHS CISO is responsible for implementing and managing the DHS-wide Information Security Program to ensure compliance with applicable Federal laws, Executive Orders, directives, policies, and regulations.

To help with these responsibilities, the DHS Office of the Chief Information Security Officer (OCISO) has the mission and resources to assist in ensuring Department compliance with information security requirements. DHS OCISO is organized into four directorates: Information Security Program Policy, Compliance and Technology, Cybersecurity Strategy, and Information Security Program Management. ISSOs will have the most interaction with the Compliance and Technology Directorate, which includes the DHS InfoSec Customer Service Center, Plan of Action and Milestones (POA&M), document review, inventory, and scorecard functions.

The DHS Information Security Program does not apply to systems that process, store, or transmit National Intelligence Information.

1.5 Essentials

The goal of information security is to help the business process owner accomplish the mission in a secure manner. To be successful, ISSOs need to know and understand the following:

- Mission and business functions of the organization (e.g., an ISSO for a procurement system should know that no maintenance or down time should be scheduled during the fourth quarter, which is extremely busy)
- How the system supports the organization's mission
- System details, including:
    - Architecture
    - System components (hardware, software, peripherals, etc.)
    - Location of each system component
    - Data flow
    - Interconnections (internal and external)
    - Security categorization

    - Security requirements
    - Configuration management processes and procedures
- Users (How many, location, etc.)
- Key personnel by name

2.0 ORGANIZATIONAL ROLES, RESPONSIBILITIES AND RELATIONSHIPS

The key to success for an ISSO is to build relationships with key personnel who have the authority or ability to ensure compliance with security laws, regulations, guidance and requirements. Key people will differ depending on circumstances. Therefore, throughout this guide, ISSOs are encouraged to coordinate with appropriate contacts as determined by their Components and different situations that arise with their systems.

This section discusses the organizational relationships between the ISSO and key personnel with whom the ISSO interfaces. It emphasizes the type of information each can provide and the suggested frequency of contact. Roles and responsibilities are included only as they are relevant to the ISSO. For a more detailed description of individual roles and responsibilities, see DHS 4300A Sensitive Systems Handbook. Sections below discuss the nature of those relationships and the types of information exchanged in each case.

Figure 1. ISSO Interactions illustrates the people the ISSO will interact with on a regular basis. Descriptions of these relationships are provided in the following sections.

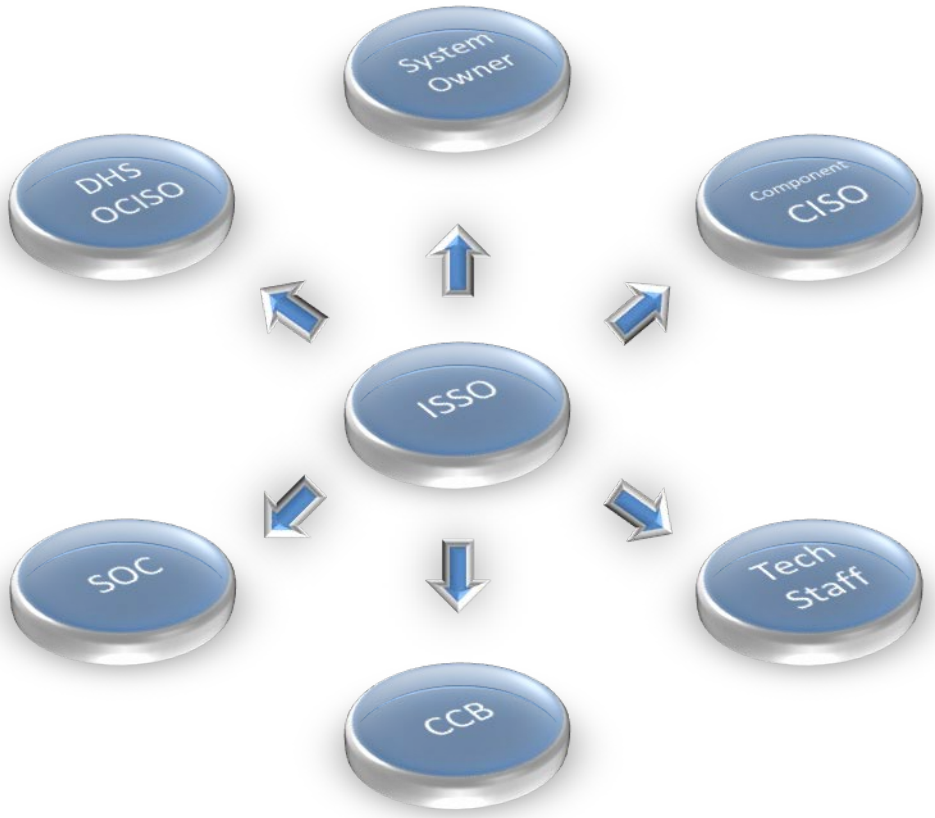

Figure 1. ISSO Interactions

2.1 DHS CHIEF INFORMATION SECURITY OFFICER (CISO)

The DHS CISO implements and manages the DHS Information Security Program to ensure compliance with applicable Federal laws, Executive Orders, directives, policies, and regulations. The DHS CISO reports directly to the DHS Chief Information Officer (CIO) and is the principal advisor for information security matters.

The DHS CISO issues Department-wide information security policies, guidance, and architecture requirements for all DHS IT systems and networks based upon guidance from NIST as well as all applicable OMB memoranda and circulars. The CISO also facilitates the development of subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems.

ISSOs are assigned duties and tasks that directly support these CISO responsibilities. Specific CISO responsibilities at the Department and Component levels can be found in the Information Security Program Roles section of DHS 4300A. The DHS CISO has several teams available to help ISSOs perform their duties and assess the effectiveness of policy, guidance, and overall program structure. In all cases, ISSOs should work through their Component CISO / ISSM and follow Component-specific procedures to request support from DHS.

DHS OCISO teams are described in detail below and include the:

- Document Review (DR) Team
- Ongoing Authorization
- Inventory Team
- Plan of Action and Milestones (POA&M) Team
- DHS InfoSec Customer Service Center

Many Components have a similar structure with an internal FISMA compliance function. Key DHS teams include those described below.

2.1.1 Document Review Team

The DHS DR Team reviews and validates Security Authorization Process documents uploaded in the Information Assurance Compliance System (IACS). The DR Team uses a checklist to ensure Security Authorization Process documents are complete and comply with DHS guidance contained in DHS 4300A, NIST Special Publication (SP) 800-53, the annual Performance Plan, and the DHS Security Authorization Process Guide. Security Authorization Process checklists are available on the DHS CISO website.

The DR team provides feedback on each package it reviews by providing the ISSO or Component CISO team with a completed DR checklist. After the checklist has been provided, the DR Team conducts a conference call with the Component to provide additional feedback, answer questions, and consider any additional information the Component may provide. ISSOs should ensure they participate in these feedback sessions along with any other stakeholders in the Security Authorization Process.

Contact with the DR team is normally made via the Component CISO/Compliance team. ISSOs should understand local requirements before contacting the DR team directly.

2.1.2 Ongoing Authorization

As stated in NIST 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, "initial system authorization is based on evidence available at one point in time, but systems and environments of operation change." To address the needs of constantly changing environments, DHS is implementing OA, which involves shifting from periodic to ongoing assessments and facilitates a continual state of awareness.

DHS implements OA in **three layers**, which collectively ensure constant control assurance.

- Layer 1: Common and Inherited Controls and Reciprocity

- Layer 2: Continuous Monitoring
- Layer 3: Event-Driven Monitoring

Event-Driven Monitoring (Layer 3) involves evaluating and testing controls when security events or "triggers" occur that may have an impact on the system's security status. Following an event, a review is conducted to determine the impact on the status of controls and risk to the system. Some key **process highlights** include the following:

- An Operational Risk Management Board (ORMB), composed of various subject matter experts, evaluates security triggers and makes risk-based recommendations.
- Following ORMB review, the CISO prepares a formal recommendation to the Authorization Official (AO) about whether or not to maintain the authorization.

Security triggers are to be reported in the Component's Trigger Accountability Log (TRAL) and provided to DHS on a monthly basis.

To qualify for OA, the following **prerequisites** must be met:

- The system must have a valid ATO.
- The information system must have a Control Allocation Table (CAT).
- The Component should have a Common Control Catalog in place.
- The Component must have a robust Continuous Monitoring program.
- The Component must assign an OA Manager.
- The Component must establish an ORMB.
- The Component must offer an OA training program.

The Component must accept and sign the DHS OA Memorandum of Agreement (MOA).

For more information about ongoing authorization, please refer to the Ongoing Authorization Methodology guide.

2.1.3 Inventory Team

The DHS Inventory Team maintains the official inventory of all DHS systems, including General Support Systems (GSSs), Major Applications (MAs), sub-systems, and minor applications. The inventory of GSSs and MAs are maintained in the IACS tool while all other sub-systems and minor applications are maintained in an off-line database at DHS. Information on sub-systems and minor applications may be obtained through the Component CISO office.

The Inventory Team in conjunction with the DHS InfoSec Customer Service Center processes all inventory change request forms and conducts the Annual Inventory Refresh effort, which focuses on maintaining an accurate inventory by conducting interviews with key personnel and investigating discrepancies. The DHS FISMA System Inventory Methodology, available on the DHS CISO webpage, provides guidance for determining system boundaries and procedures for submitting change requests.

2.1.4 Plan of Action and Milestones (POA&M) Team

The DHS POA&M Team is responsible for monitoring the status of POA&Ms, assisting Components in improving the quality and effectiveness of their POA&Ms, and providing POA&M guidance.

The DHS POA&M Team is available for POA&M training and Assist Visits that can be requested through the Component CISO to the DHS InfoSec Customer Service Center. Training can cover a range of topics. Assist Visits usually involve Subject Matter Experts (SMEs) from DHS working with small groups at the Component to deal with specific issues, such as developing POA&Ms for audit findings or using IACS reports. Assist Visits can be used to help develop real POA&Ms based on real vulnerabilities.

ISSOs should be thoroughly familiar with DHS 4300A, Attachment H, POA&M Process Guide.

2.1.5 DHS InfoSec Customer Service Center

The DHS InfoSec Customer Service Center provides help desk-type support for the IACS tool (e.g., reset passwords) and serves as the focal point for questions about the DHS Information Security Program or any of its elements (e.g., DR, inventory, POA&M, etc.). Services provided include account maintenance, PO&AM support, Document Review and FISMA guidance as well as review and implement FISMA Inventory change requests. The DHS InfoSec Customer Service Center has access to a variety of Subject Matter Experts (SMEs) and can provide an authoritative response to questions regarding the DHS Information Security Program. ISSOs should use the chain of command and resources within their Component to try to resolve questions but should not hesitate to use the DHS InfoSec Customer Service Center as a resource when needed.

2.2 Component CISO / ISSM and Staff

The Component CISO team should be a primary source of information and assistance for all ISSOs. ISSOs should become familiar with the organization and people in their CISO office so they can request assistance when needed. Often, the Component CISO staff can provide specific answers to questions about the Security Authorization Process, POA&Ms, requirements, the IACS tool, training, policies and procedures, and where else to go to get answers. In some cases, the CISO office may even provide resources to help with specific issues (e.g., scans, Security Assessment Plans, etc.).

The Component CISO team is also the principle conduit for all requests to DHS OCISO for training, document reviews, or other support. All requests for support or questions concerning policy or implementation of security controls must be routed through the CISO or designated representative. DHS will process requests for the following only when submitted by the Component CISO or designee:

- IACS access
- ISSO Training
- Waivers and exceptions

- Security Authorization Process document review

2.3 System Owner

System Owners (SO) use information technology to help achieve mission needs within their program area of responsibility. ISSOs are responsible for supporting their SOs to ensure they understand security requirements and implications of not meeting them. The ISSO's goal should be to help the SO operate the system as securely as possible to fulfill mission requirements. However, SOs are ultimately responsible for the security of their systems and must ensure that each of their systems is deployed and operated in accordance with DHS policy and guidance.

The SO is the ISSO's primary source of information and resources. In most cases, the ISSO works directly for and reports to the SO. ISSOs should maintain frequent, if not daily, contact with their SOs.

SOs are responsible for designating an ISSO in writing for each information system under their purview. See Section 5.1 for additional information on ISSO letters.

2.4 System, Database, and Major Application Administrators (Technical Staff)

Technical staff are directly responsible for implementing most technical security controls. System security cannot be effective without their active participation. Conversely, technical staff focus on ensuring the system is available for their users and can also be a primary source of vulnerabilities. ISSOs should know key technical personnel for their systems by name and should coordinate with them frequently as part of the continuous monitoring process.

Technical staff are a primary source of information for the Security Authorization Process, annual assessments, audits, determining whether Information Security Vulnerability Management (ISVMs) messages are applicable and addressed, Contingency Plans and tests, training, and a number of other issues.

2.5 Business Owner

The Business Owner has different functions within each Component or organization. In general, business owners are responsible for ensuring the mission of the organization is accomplished. In some cases, business owners are responsible for funding and other resources that support their line of business. Although ISSOs will seldom interface with the business owner, it is important they understand the organization's business functions to help ensure business is conducted as securely as possible. For example, an ISSO for a procurement system should know maintenance or down time should not be scheduled during the fourth quarter of the fiscal year because of the criticality of the support functions.

2.6 Security Control Assessor (SCA)

A Security Control Assessor (SCA) (formerly Certifying Official) is a senior management official who verifies the results of the security assessment and makes an authorization recommendation to the Authorizing Official (AO). Even if ISSOs are not conducting the

Security Authorization, they will have a role in providing data and coordinating activities. It is essential for ISSOs to coordinate with their SCA at the initial Security Authorization and throughout the system lifecycle to ensure they understand requirements, schedules, and processes.

2.7 Authorizing Official

The AO formally assumes responsibility for operating an information system at an acceptable level of risk. The DHS CIO serves as the AO for all enterprise systems or designates an AO in writing. The Component CIO serves as the AO for Component information systems or designates one in writing. The DHS Chief Financial Officer (CFO) serves as the AO for CFO designated financial systems managed at the DHS level. The Component CFO is the AO for CFO designated financial systems managed by the Component.

ISSOs generally have limited interaction with their AOs except during the Security Authorization Process and whenever there is a need to accept risks. In most cases, ISSOs will interact with their AO through the SCA or follow Component-specific processes. In either case, ISSOs should ensure they understand the AO's expectations and the process for presenting the ATO letter for signature early in the Security Authorization Process.

ISSOs should also brief the AO whenever there is a significant change to system risk or system design that could require a re-accreditation.

2.8 Chief Financial Officer

The DHS CFO implements and manages the DHS Financial Program, including oversight of DHS financial systems. The DHS CFO designates financial systems and oversees security control definitions for financial systems (See section 6.2).

The DHS or Component CFO is the AO for only CFO designated financial systems managed at their level.

ISSOs will interface with CFO staff during preparations for the Security Authorization Process, audits, and during remediation of weaknesses identified during financial audits or internal reviews. ISSOs may have to provide the CFO reports on the status of remediation of weaknesses at various times throughout the year.

2.9 Chief Privacy Officer

The DHS Chief Privacy Officer implements and manages the DHS Privacy Program, including creating and ensuring compliance with privacy policy. The DHS Chief Privacy Officer assists the Component Privacy Officers and Privacy Points of Contact (PPOC) with policy compliance at the Component level. The Chief Privacy Officer's responsibilities of interest to ISSOs include:

- Oversee privacy incident management
- Review and approve program and system Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), and System of Records Notices (SORNs)

- Designate Privacy Sensitive Systems based on validated PTAs. Privacy Sensitive Systems are those that maintain Personally Identifiable Information (PII)

ISSOs will have limited interface with Privacy personnel except when there is an incident or during the Security Authorization Process when the Privacy Office must review and approve the system's PTA. Component Privacy Offices follow Component-specific procedures.

With the introduction of NIST (SP) 800-53 Revision 4, privacy controls have been added. These controls are under the authority and responsibility of the Privacy Office. ISSOs do not address or modify these controls.

2.10 Chief Security Officer (CSO) / Facility Security Officer (FSO)

The DHS/Component CSO implements and manages the DHS/Component Security Program for DHS facilities and personnel. ISSOs will not normally interface with the CSO but may need information from the CSO's office regarding policies, procedures, or controls that deal with physical or personnel security. The FSO will be able to provide detailed data regarding personnel and physical access controls within a specific facility or unit (e.g., data center) as well as information on environmental controls.

2.11 DHS Security Operations Center (SOC)

The DHS SOC is the central coordinating and reporting authority for all Sensitive and National Security computer security incidents throughout the Department. The DHS SOC exchanges information with Component SOCs, Network Operations Centers (NOCs), the Homeland Secure Data Network (HSDN) SOC, the Intelligence Community, and external organizations in order to facilitate the security and operation of the DHS network.

While the DHS SOC has overall responsibility for incident management and reporting, each Component has its own SOC capability and procedures for dealing with incidents. **It is critical for ISSOs to know and understand their Component's policies and procedures regarding incident reporting and handling.** ISSOs will usually serve in a key role in the event of security incidents. This role varies depending on circumstances and Component-specific procedures but could include responding to the incident, reporting the incident, investigating the cause of the incident, or remediating vulnerabilities discovered as a result of the incident. Other SOC functions (both at the DHS and Component levels) that are useful to ISSOs include:

- Provide ISVM messages
- Initiate necessary investigations
- Notify appropriate law enforcement authorities, if required
- Provide scanning services
- Provide forensics capabilities

2.12 Configuration Control Board (CCB)

ISSOs should be involved in the change control process for a number of reasons. ISSOs should be a member of the CCB with responsibility for their system and have input to proposed changes

and their impact on system security. Even if not directly involved with the process, ISSOs need to be aware of any system changes affecting system security could require updates to the Security Plan (SP) other system documents, or could affect Interconnection Security Agreements (ISAs) or other interconnection issues. The ISSO should make every effort to be involved in the change control process by attending CCB meetings. For systems in development, ISSOs should attend the change review meetings to ensure security acceptance before the system is moved through the CCB.

2.13 Facility Managers

Facility managers can be an invaluable source of information regarding common or inherited controls, especially in the areas of environmental and physical controls. While ISSOs may not interact directly with facility managers, they should identify and develop a relationship with appropriate Points of Contact (POCs) at facilities hosting their systems. Such POCs may include the facility ISSO, technical staff supporting their system, and physical or access control staff.

2.14 Peers

One of the best sources of information and support for ISSOs are their peers. ISSOs should get to know other ISSOs who have similar systems or who are assigned to GSSs that support their systems. Building relationships with other ISSOs can prove invaluable when sharing best practices or asking simple "How do I …?" or "Who do I call…?" questions. Becoming familiar with other Component ISSOs or with the ISSOs of a GSS will also facilitate communication for understanding how to identify and respond appropriately to inherited controls in security documents.

3.0 ISSO RESOURCES AND TOOLS

To be successful, an ISSO needs to be aware and take full advantage of available resources. The following sections describe references, tools and other resources ISSOs should include in their arsenals.

3.1 References

The best advice to any ISSO is to read the directions first. Almost every task an ISSO must accomplish has some form of guide or Standard Operating Procedure (SOP). The documents listed below are the basic references an ISSO should be familiar with. ISSOs should know what each document contains and know where to look when questions arise. Additionally, ISSOs should be thoroughly familiar with their Component guidance, which often expands on or tailors the guidance listed below. As a result, Component specific guidance should be the primary source of information used by ISSOs. Key reference documents are described in the subsequent sections.

3.1.1 NIST Special Publications

NIST Special Publications in the 800 series are of general interest to the computer security community. There are more than 100 NIST Special Publications relating to everything from the Security Authorization Process to specific guides for implementing various technology solutions

(e.g., Bluetooth, Secure Web Services, etc.). They serve as the basis for DHS and Component security policies and procedures. However, ISSOs need to be aware DHS has tailored NIST guidance for application within the Department. While NIST should be used to provide general guidance, ISSOs should rely on Department and Component specific guidance.

While most NIST Special Publications are useful as general references, NIST SP 800-53: *Recommended Security Controls for Federal Information Systems* and NIST SP 800-53A: *Guide for Assessing the Security Controls in Federal Information* Systems are two of the most important for ISSOs. They contain detailed explanations of information security controls and the test cases used to assess them. All ISSOs should be thoroughly familiar with both of these documents. NIST SPs are available at http://csrc.nist.gov/publications/PubsSPs.html.

3.1.2 DHS CISO Website

The DHS CISO website has all the Department-level references an ISSO needs to perform most tasks. ISSOs should be familiar with the site and its contents. The following sections list key documents on the site.

3.1.3 DHS 4300A

The DHS Sensitive Systems Policy Directive 4300A and DHS 4300A Sensitive Systems Handbook serve as the authoritative guidance for implementing information security within DHS. The Sensitive Systems Handbook has more than 20 attachments ISSOs should be aware of. Some of the most commonly used attachments include:

- Attachment B, Waivers and Exceptions: contains the DHS Waivers and Exceptions Request form with instructions on how to complete and submit the request
- Attachment C, ISSO Letter: contains a sample designation letter for an ISSO/Assistant ISSO
- Attachment F, Incident Response: defines and documents DHS incident management policy, requirements, procedures, and guidance for DHS Components and Headquarters in the management and reporting of cyber security incidents
- Attachment G, Rules of Behavior: provides sample general rules of behavior that apply to all users of DHS systems and IT devices
- Attachment H, POA&M Process Guide: describes the POA&M process and provides detailed guidance regarding how to develop a POA&M
- Attachment N, Interconnection Security Agreements (ISA): provides guidance on developing an Information Security Agreement (ISA) and a sample format as well as a summary of Memorandums of Understanding / Agreement (MOU/MOAs)
- Attachment O, Vulnerability Management: defines and documents the DHS Information Security Vulnerability Management (ISVM) program requirements, procedures and guidance for all Components. It includes procedures for participation and management of the program as well as reporting requirements

3.1.4 DHS Information Security Performance Plan

The annual performance plan provides details defining how each score is computed for the Department's monthly scorecard.

3.1.5 DHS Information Security Categorization Guide

This guide provides guidance for completing the FIPS-199 and E-authentication workbooks as well as the Privacy Threshold Analysis (PTA).

3.1.6 Federal Information Processing Standards (FIPS) 199 Workbook

This workbook is used to identify security categories of information and information systems for confidentiality, integrity, and availability.

3.1.7 E-Authentication Workbook

This workbook is used to determine if an E-Authentication risk assessment is required.

3.1.8 Privacy Threshold Analysis (PTA) Template

This template is used to determine and document whether a Privacy Impact Assessment (PIA) is required.

3.1.9 DHS FISMA System Inventory Methodology

The DHS FISMA System Inventory Methodology describes the methodology used by DHS to maintain a consistent, Department-wide inventory of information systems.

3.1.10 DHS Security Authorization Process Guide

The DHS Security Authorization Process Guide provides practical assistance for completing the Security Authorization Process within the Department. It identifies documents that must be included in the Security Authorization Package and guidance regarding the content and level of detail that is required.

3.1.11 DHS CISO NIST SP 800-53 Security Controls Tri-fold

DHS has adapted the NIST concept of categorizing systems based on the "high water mark" for confidentiality, integrity, and availability. At DHS, required controls are based on the category in each of the three security objectives areas, confidentiality, integrity, and availability. The DHS CISO NIST SP 800-53 tri-fold identifies which controls are required based on the categorization of each objective area. The tri-fold also identifies key controls for CFO designated financial systems and privacy systems.

3.1.12 Sensitive Systems Configuration Guidance

The DHS CISO website has a number of configuration guides that should be used to harden system components (e.g., Cisco Routers, Oracle databases, HP-UX, Windows, etc.). Appendix A contains a list of available guides.

3.1.13 Ongoing Authorization Guidance

The DHS OCISO has authored a guide for Ongoing Authorization. This guide is available upon request.

3.1.14 Common Control Guidance

The DHS OCISO has authored a guide for Common Control Catalog creation, distribution, and usage. This guide is available upon request.

3.1.15 DHS CPIC Guidance

The DHS CPIC guide, provides information regarding the CPIC process. The CPIC process integrates strategic planning, enterprise architecture, portfolio management, privacy, security, budgeting, procurement, and the management of assets.

3.1.16 OMB Memoranda

Every year OMB publishes a Memo with reporting instructions and guidance for FISMA (e.g., M-09-29, FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management). DHS interprets these Memos and incorporates new guidance in the annual performance plan, but ISSOs should be aware of them as their content should provide insight into new requirements and scorecard metrics. Memos are available at: http://www.whitehouse.gov/omb/memoranda_default/

3.1.17 OMB Circulars

There are a number of OMB Circulars that provide general guidance on information security. Three of the most relevant are:

- A-130 - Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources
- A-123 - Management's Responsibility for Internal Control
- A-127 - Financial Management Systems

OMB A-130 applies to all IT systems while A-123 and A-127 apply primarily to financial systems. ISSOs should be aware of these foundation documents and have a general understanding of their content. They can be found at: http://www.whitehouse.gov/omb/circulars_default/

3.1.18 IACS

The IACS tool collects and organizes FISMA-related data. DHS requires the use of IACS for creating POA&Ms, completing control assessments, and documenting the Security Authorization Process activities. Additionally, the DHS FISMA system inventory is stored in IACS. The FISMA inventory in IACS includes only General Support Systems (GSS) and Major Applications (MA). Subsystems and minor applications are maintained offline in a separate data base. In the future, all inventory systems, including subsystems and minor applications, will be housed in IACS.

IACS serves as the repository for compliance related information which includes, but is not limited to the following types of information:

- Status of all Component security programs and their compliance with DHS metrics
- POA&Ms

- Assessments for each system
- Security Authorization artifacts and their approval status
- Official DHS Information System Inventory
- Contact information for each DHS system

IACS also has a number of reports that can be run to check on the status of many items the ISSO is responsible for. It is one of the ISSO's key security management resources.

IACS is the primary source of information used to compile FISMA reports that the Department is required to submit to OMB and Congress, as well as the monthly scorecard presented to the CIO Council and CISO Council. Thus, it is important that data in IACS is accurate and current to avoid a negative impact on any of these reports.

IACS is also used to conduct a security authorization and support the security authorization process. All work on the security authorization process is performed in the tool. Security authorization process documents are generated when the ISSO 'publishes' the document in IACS. The documents contained within IACS include:

- Security Plan (SP)
- RTM
- Risk Assessment
- Vulnerability Report
- Contingency Plan
- Contingency Plan Test
- Security Assessment Plan
- Security Assessment Report
- POA&M Report
- ATO Letter

For more information on using IACS, please refer to the Security Authorization Guide.

3.1.18.1 Requesting IACS Accounts and Training

IACS account requests are made via the Component CISO or designated Point of Contact (POC) to the IACS Portal page. The following information is required to obtain an account:

- First and last name
- Email address
- Phone number
- Role Requested (e.g., Component CISO, ISSO, Security Analyst)
- Component

- System and program

The Component CISO or designated POC is responsible for ensuring the names submitted for user accounts are valid users, are eligible for access to DHS information systems, and have a valid need to access the systems. They are also responsible for ensuring accounts that are no longer valid are reported to the DHS InfoSec Customer Service Center.

Training for IACS should be requested via the Component CISO or designated Point of Contact (POC) to the DHS InfoSec Customer Service Center.

3.2 DHS InfoSec Customer Service Center

The DHS InfoSec Customer Service Center is available to answer questions during normal business hours from 7:30 AM to 5:30 PM via telephone or e-mail. The Customer Service Center serves as a conduit for questions regarding the DHS Performance Plan/scorecard and any other DHS information security process (e.g., document review, POA&M, etc.). The Customer Service Center will also coordinate training or assistance visits for scorecard, POA&M, the Security Authorization Process, or other topics as needed.

InfoSec Customer Service Center may be reached at:

- Email: isosupport@hq.dhs.gov
- Phone: (202) 343-2500

4.0 SYSTEM ENGINEERING LIFE CYCLE (SELC)

The SELC methodology provides a structured approach to managing information systems projects. It also allows introduction of information security planning, including budgeting, review, and oversight. The SELC process begins with the Program Authorization decision within the Capital Planning and Investment Control (CPIC) process. The CPIC process (MD 4200), as described in the DHS CPIC Guide, integrates strategic planning, enterprise architecture, portfolio management, privacy, security, budgeting, procurement, and the management of assets.

There are eight distinct phases in the SELC as depicted in Figure 2. SELC Process.

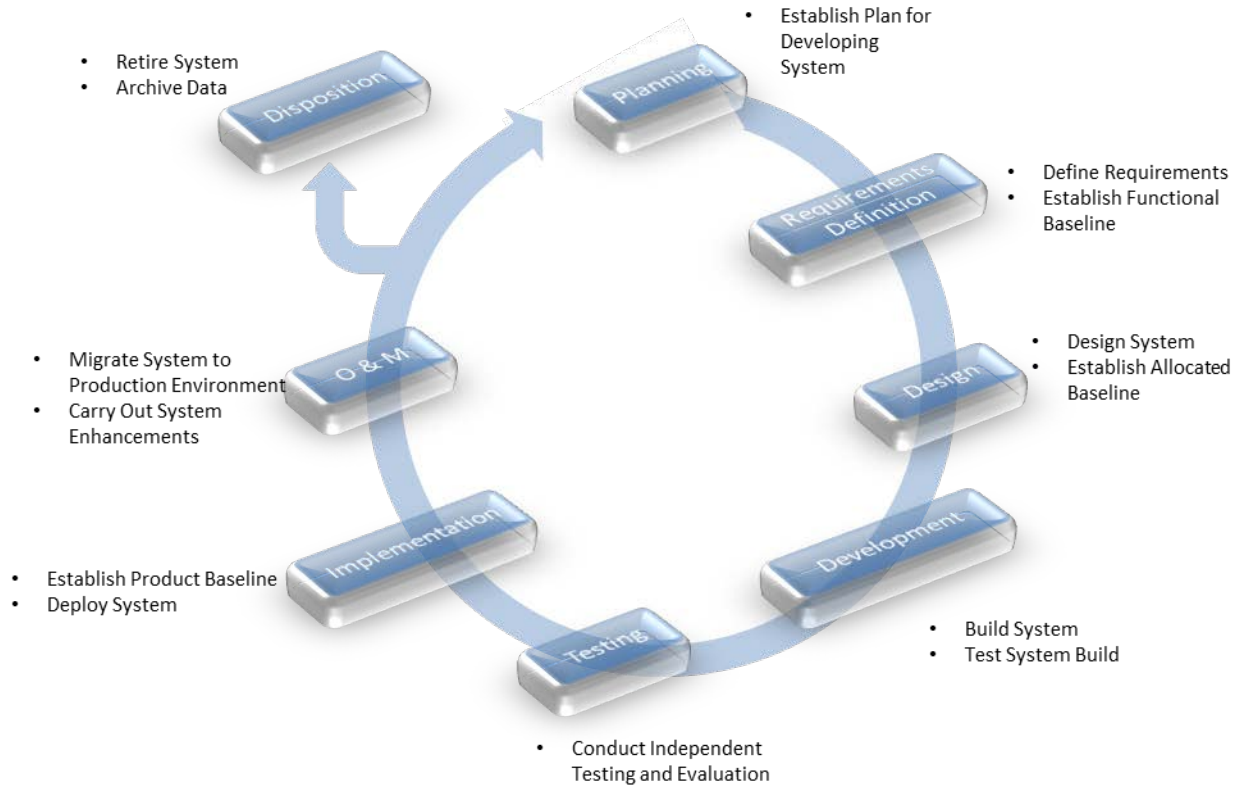

Figure 2. SELC Process

Information security is an integral part of the system life cycle with tasks performed in each life cycle phase. ISSOs should familiarize themselves with both the Component's and DHS's SELC. The DHS SELC describes each phase of the development lifecycle and the security activities that should take place. The SELC makes it clear that information security is an integral part of the lifecycle process from planning through disposition. It is important for ISSOs to make every effort to attend the meetings that move the system from one phase to another.

4.1 Life Cycle Phases

4.1.1 Planning

The Planning Phase defines the system concept from the user's perspective and establishes a comprehensive plan for developing the system. Information security activities include the following:

- Preparation of the initial Risk Assessment and Security Plan

- Ensuring that adequate budgetary resources for information security requirements are available (This is a SO responsibility but it is incumbent on the system ISSO to ensure resources are available)
- Ensuring that appropriate security requirements are included in contracts if the development is to be outsourced

ISSOs are rarely assigned during this Phase but must complete these activities whenever they become involved in the life cycle.

4.1.2 Requirements Definition

During the Requirements Definition Phase, users and technical staff define detailed requirements to ensure the system will meet user requirements. This results in the establishment of a Functional Baseline. Information security activities include:

- Updating the Risk Assessment and Security Plan
- Creating an RTM in IACS and reviewing IT Baseline Security Requirements
- Developing an initial Plan of Action and Milestones
- Developing an initial Security Assessment Plan
- Reviewing information security budget requirements
- Preparing the initial security inputs to the IT Training Plan
- Preparing the initial Contingency Plan

Security requirements must be included in the functional baseline to ensure appropriate security controls can be included in the system design. It is much easier and more cost effective to include security controls at this stage rather than adding them in later. In some cases, required controls cannot be added after the design has been completed due to design constraints.

4.1.3 Design

The system development then moves to the Design Phase, during which the requirements are transformed into detailed design specifications. During the Design Phase, an Allocated Baseline is established and documented in the System Design Document. Information security activities include:

- Updating the Risk Assessment and Security Plan
- Reviewing budget requirements
- Developing Interconnection Security Agreements
- Updating the security information in the IT Training Plan
- Updating the Contingency Plan
- Preparing the initial Security Authorization Package

During the Design Phase, ISSOs must ensure the design is compliant with security requirements. For example, if the design includes an encryption capability, ISSOs should ensure the solution chosen is FIPS 140-2 compliant. ISSOs should also be aware of potential new requirements and ensure the design is flexible enough to accommodate them in the future.

4.1.4 Development

After formal approval of the design, the project enters the Development Phase. During this phase, the development team builds the system according to the design specified during the Design Phase and conducts development testing. The Development Phase represents an iterative process during which the development team builds the system, tests the system build, modifies the system based on any problems identified during Development Testing, and then tests the modified system build. Information security activities include:

- Conducting the initial Developmental Security Assessment Plan
- Updating the Risk Assessment and Security Plan
- Developing the initial Operational Security Assessment Plan
- Reviewing budget requirements
- Updating the Security Authorization Package

During the Development Phase, ISSOs ensure the development environment has proper controls, including configuration management and physical access controls. For example, Development environments sometimes have uncontrolled connectivity to production systems but are not included in the accreditation boundaries.

4.1.5 Test

When the developed system is fully functional and has successfully passed Development Testing, the system development project moves into the Test Phase. During this phase, independent testing and evaluation is conducted to ensure the developed system functions properly, satisfies the requirements (including security requirements) developed in the Requirements Definition Phase, and performs adequately in the host environment. Information security activities include:

- Conducting formal Developmental Security Assessment Plan
- Reviewing budget requirements
- Updating the Risk Assessment and Security Plan
- Updating the Security Authorization Package

> ⚠ **Systems must have a signed ATO before becoming operational.** "Operational" means the system is processing real or operational data. Systems described as a "prototype" or "proof of concept" are "operational" if they process real data.

ISSOs should ensure sensitive operational data is not used in testing without proper security controls. If test or sanitized data is not available for testing, Authorizing Officials (AOs) may

grant an Interim Authority to Operate (IATO) for systems that are undergoing development testing or are in a prototype phase of development. A system must obtain an Authority to Operate (ATO) prior to passing the Key Decision Point 3 milestone in the development life cycle. The AO may grant an IATO for a maximum period of 6 (six) months and may grant one extension for six month extension. IATOs are not appropriate for operational systems.

4.1.6 Implementation

The system development project enters the Implementation Phase after the system has successfully passed testing and is ready for deployment. The output of this phase is the Product Baseline, which consists of the production system, databases, an updated data dictionary, associated infrastructure, and supporting documentation. During this phase the system is deployed to designated production sites. Information security activities include:

- Conducting the Operational Security Assessment Plan
- Reviewing adequacy of budget requirements
- Finalizing the security inputs in the Training Plans
- Updating the Risk Assessment and Security Plan
- Finalizing the Security Authorization Package

4.1.7 Operations and Maintenance (O&M)

After the system has been successfully deployed, it enters the O&M Phase. During this phase, the system becomes operational and any necessary system modifications are identified and documented as "System Change Requests." These changes must be formally approved before they can be implemented. Information security activities include:

- Reviewing the Security Authorization Package status and maintaining the currency of the documentation
- Conducting Annual Assessments to ensure security controls remain effective over time
- Monitoring the status of remediation activities through the POA&M process
- Conducting annual user security awareness training and role-based training (e.g., training for ISSOs, AOs, network and system administrators, managers)
- Maintaining adequate budgetary resources

4.1.8 Disposition

Finally, the system is retired from the operational environment during the Disposition Phase. Activities during this phase involve:

- Terminating system operations
- Removing the system from the production

The FISMA inventory makes a distinction between "decommissioning" and "disposal." Decommissioning is the process of removing the system from the production environment (i.e., unplugging it). Disposal means all media has been sanitized and the system is no longer in the inventory.

environment

- Archiving the system components, data, and documentation
- Disposing of equipment and media in accordance with security requirements
- ISSOs need to be aware of system components that may be replaced before the Disposal Phase and ensure they are properly sanitized

4.2 ISSO Responsibilities during the Life Cycle

Ideally, ISSOs become involved with their systems early in the lifecycle to identify security requirements and provide input to the system design to ensure the proper controls are built-in and do not need to be added later, which is usually more expensive and often not possible. Unfortunately, it is not unusual for an ISSO to be assigned to a system just before it becomes operational and the ATO is due. However, joining the system development process late in the game does not reduce the ISSO responsibilities. It requires only that the same requirements be completed in a shorter period. Overall ISSO responsibilities include:

- Participate in planning and executing the SELC process
- Provide information security expertise to system development teams
- Prepare, review or comment on all SELC security documents
- Ensure appropriate security controls are applied during each SELC Phase (e.g., software CM)
- Ensure test data is used during system testing
- Conduct continuous monitoring during Operations and Maintenance Phase, to include
  - Maintenance of a current ATO
  - Monitoring compliance
  - Conducting Annual Assessments
  - Conducting periodic scans
  - Conducting audit log reviews
  - Ensuring media is properly sanitized prior to disposal

5.0 ISSO RESPONSIBILITIES

The ISSO serves as the principal advisor to the information system owner and the CISO/ISSM on all matters (technical and otherwise) involving the security of the information system. The ISSO typically has the detailed knowledge and expertise required to manage the security aspects of the information system and, in many cases, is assigned responsibility for the day-to-day

⚠ While the ISSO performs security functions, the SO always has overall responsibility for information system security.

security operations of the system. This responsibility may also include, but is not limited to, physical security, personnel security, incident handling, and security awareness and training. The ISSO may be called upon to assist in the development of the system security policy and to ensure compliance with the policy on a routine basis. In close coordination with the information system owner, the ISSO often plays an active role in developing and updating the Security Plan as well as managing and controlling changes to the system and assessing the security impact of those changes. The ISSO also coordinates with external agencies and assists in the preparation of the ISA to ensure all external connections meet protection requirements and are documented in the Security Plan, Risk Assessment, and security operating procedures.

DHS policy regarding ISSO responsibilities is provided below.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.8.a	An ISSO shall be designated for every information system and serve as the point of contact (POC) for all security matters related to the system.	PL-1
2.1.8.b	An ISSO shall ensure the implementation and maintenance of security controls in accordance with the Security Plan (SP) and DHS policies.	PL-1
2.1.8.c	An ISSO may be a DHS employee or a contractor.	PL-1
2.1.8.d	An ISSO may be assigned to more than one system.	PL-1
2.1.8.e	ISSO duties shall not be assigned as collateral duties unless approved by the Component CISO.	PL-1
2.1.8.f	The ISSO shall have a clearance greater than or equal to the highest level of information contained on the system. The minimum clearance for an ISSO shall be Secret.	
2.1.8.g	The ISSO shall ensure that timely responses are provided to Infrastructure Change Control Board (ICCB) change request packages.	

The following sections discuss the most common ISSO responsibilities and required actions. Discussion topics generally correspond to NIST Special Publication (SP) 800-53 families and NIST guidance is clarified or explained within the DHS ISSO context, as necessary. Some specific topics of interest to ISSOs are broken out separately. Specific, non-NIST issues are also identified in each section as appropriate.

5.1 ISSO Letter

All ISSOs must be designated in writing following the guidance in DHS 4300A, Attachment C. ISSO letters define duties and responsibilities and are usually signed by the SO. ISSO letters must be updated whenever a change occurs and a current letter must be uploaded in the IACS

tool as part of the Security Authorization Package. The designated ISSO should be identified consistently in three sources: the ISSO letter, the SP and in the FISMA Inventory.

5.2 Access Control

ISSOs may or may not have a direct role in controlling access to systems, but all ISSOs have an oversight responsibility to ensure proper access controls have been implemented for both system access and physical access to data processing facilities. Access controls apply to federal employees, contractors, and anyone else who has access to DHS systems or data.

5.2.1 System Access

ISSOs must ensure processes are in place to ensure:

- Unused or inactive accounts are reviewed and deactivated monthly. Accounts are considered to be unused if no login has occurred within 30 days for FIPS 199 high systems, 45 days for moderate systems and 90 days for low systems
- Users have completed a background investigation and receive initial security awareness training before being granted system access
- The user's supervisor authorizes the system and levels of access the user requires
- The SO approves user access privileges
- User access is validated periodically by an authorized supervisor to ensure the user requires continued access to the system and the correct privileges are assigned. These reviews must take place at least annually but should occur more frequently as resources permit
- All departing employees have their access privileges terminated immediately. Termination of access privileges also applies to employees whose job functions have changed to ensure they no longer require access to the level to which they were previously granted
- Authority to add, change, or remove component devices, dial-up connections, and network addresses and protocols, or to remove or alter programs, be tightly controlled with access limited to only a select group of authorized personnel
- All methods of remote access (e.g., dial-up, Internet), including remote access for privileged functions, is strictly controlled and only a limited number of users are authorized
- Separation of duties is enforced through technical (e.g., Role Based Access Control (RBAC)) or manual means (e.g., supervisor authorization)
- Accounts are locked after three consecutive invalid access attempts
- Users are prohibited from using personally owned computers or devices systems for official U.S. Government business involving the processing, storage, or transmission of federal information

- Signed Rules of Behavior (ROB) are completed for each user account

5.2.2 Physical Access

ISSOs generally do not have direct control over physical access policies or procedures but are still responsible to ensure physical access controls are in place and effective. ISSOs should review policies and procedures for access to spaces where their IT assets are hosted or used (i.e., end-user space) and verify procedures are being followed by visiting all relevant facilities. Locations to be visited include end-user workspace, facilities where IT assets are housed, alternate processing sites and off-site storage facilities.

5.3 Acquisition Process

ISSOs should work with SOs and program managers to ensure all procurement actions take security requirements into account and Statements of Work (SOWs) have appropriate language to avoid security-related problems in the future. Additionally, knowledge of the acquisition process is essential to meeting NIST controls SA-4 and SA-9. Two sources that will help ISSOs meet these requirements are the Department of Homeland Security Acquisition Regulation (HSAR) and the Information Technology Acquisition Review (ITAR) process.

5.3.1 Department of Homeland Security Acquisition Regulation

The HSAR establishes uniform Homeland Security policies and procedures for all acquisition activities throughout the Department, except within the TSA. The HSAR includes a number of security clauses that should be included in all contracts to help Program Managers and Contracting Officers address basic security requirements. The most relevant clauses include:

- Clause **3052.204-70** which provides security requirements for unclassified information technology resources. This section directs the Contractor to:
    - Be responsible for IT security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location
    - Provide, implement, and maintain an IT Security Plan which will describe the processes and procedures to ensure appropriate security of IT resources
    - Return all sensitive DHS information and IT resources and certify all non-public DHS information has been purged from any contractor-owned system at the expiration of the contract
    - Submit written proof of IT Security accreditation in accordance with DHS Sensitive System Policy Publication, 4300A, within 6 months after contract award
- **Clause 3052.204-71** which addresses Contractor employee access. It requires that before receiving access to IT resources or sensitive information, the individual must:
    - Be a U.S. citizen or have a waiver
    - Have a favorably adjudicated background investigation
    - Receive a security briefing
    - Complete any nondisclosure agreement furnished by DHS

5.3.2 Information Technology Acquisition Review

To assist in these responsibilities, DHS has implemented an ITAR process to ensure IT acquisitions are compliant with the DHS Security policies, Enterprise Architecture, Investment Strategy, Section 508 of the Rehabilitation Act, and are in alignment with DHS goals and portfolio implementation. ISSOs should be aware of this process and participate in or coordinate with any reviews for their systems.

DHS Management Directive (MD) 0007.1: *Information Technology (IT) Integration and Management* establishes DHS's vision, authorities, and responsibilities of the Department's and Components' CIO. This MD mandates any proposed IT acquisition of $2.5M and above be reviewed and approved by the DHS CIO. Information Technology acquisitions are defined as services for IT, software, hardware, communications, and infrastructure.

The ITAR Quick Essentials Guide is intended to provide DHS Program Managers with insight to help them navigate the ITAR process and better align their IT acquisitions with DHS policy and guidelines. From the initial submission through the resolution of conditions placed upon a request, this guide addresses some of the more common mistakes that can occur along the way.

5.4 Control Assessments

As part of the Continuous Monitoring phase of the Security Authorization Process, ISSOs are responsible for conducting assessments of controls for their system to ensure the controls have been implemented properly and are still effective. Even if properly implemented, control effectiveness may become degraded over time due to changes in the IT environment or other factors. Therefore, it is critical to reassess their effectiveness periodically.

The ISSO conducts assessments using test cases identified in NIST SP 800-53A and documents results. The number of controls assessed varies depending on whether the system is undergoing security authorization, is within a current ATO cycle, or is under Ongoing Authorization (OA). All systems that are not under OA require annual assessments, which must be completed within 12 months of the ATO-anniversary date.

New systems or systems undergoing security re-authorization require an annual assessment be completed for 100 percent of controls as a baseline for future efforts. The annual assessment for these systems generally reflects the results of the Security Assessment Plan.

Systems within the current ATO cycle and not undergoing OA are required to test only 33% of their applicable controls. The 33% is based on the total applicable controls per DHS tailoring guidance for confidentiality, integrity, and availability (see the DHS CISO NIST SP 800-53 Security Controls Tri-fold). For example, a Low/Low/Low system is required to assess only 33% of NIST Special Publication (SP) 800-53 controls. The 33% of controls tested must include:

- All DHS designated Key Controls
- All new controls, whether NIST or 4300A updates

- Non-overlapping and non-inherited controls (i.e., inherited controls do not count for the 33%)

Key controls are identified in the DHS Information Security Performance Plan and are based on a number of factors including known threats, department level trends, and senior management priorities. Key controls require artifacts be in the IACS tool to validate the control has been satisfied. All relevant artifacts providing evidence of the recent test of the control are acceptable. For example, a memo documenting the date of testing is acceptable. Artifacts should include a summary or evidence that a review was conducted but contain no actual system data. Sample control artifacts are provided in the DHS Information Security Performance Plan.

Any control not fully satisfied (i.e., fails one or more test cases) must be included in a POA&M for remediation.

5.5 Annual Security Awareness and Role-based Training

A key objective of information security awareness and role-based training is to ensure all DHS personnel (employee, detailee, military, or contractor) understand their roles and responsibilities within the enterprise and are adequately informed as to how to perform on the job. ISSOs should check with their CISO office to determine how annual security awareness training and role-based training is conducted and documented Component-wide. Within Component-specific guidelines, ISSOs are responsible for ensuring:

- All system users receive security awareness before being granted system access
- All system users receive security awareness annually
- All system users receive additional security awareness whenever system security changes occur, or when the user's responsibilities change
- Personnel with significant security responsibilities receive annual specialized role-based training specific to their security responsibilities; positions include ISSOs, network administrators, system administrators, SOs, database administrators, IT Project Managers, and AOs
- User accounts, including access to email, are disabled for users who do not complete the annual security refresher course
- A record of security awareness and role-based training is maintained to include the name and position of the person trained, the type of training, the date of the training, and the cost of the training
- Statistics on initial and refresher security awareness are submitted to the Component CI Training requirement summary
- Personnel with Contingency Plan responsibilities receive annual refresher training for high and moderate availability systems (no training is required for Low availability systems)

- All personnel receive Incident Response Training at least annually; incident response training should be coordinated with the Component SOC and local training office and may be incorporated into annual refresher training

5.6 Audits

Numerous IT systems are subject to audits throughout the year for various purposes. Information security audits are a review of system controls usually conducted by an entity independent from those operating or maintaining the system. They are similar in some ways to a Security Assessment Plan. Most audits of DHS IT systems are performed by the DHS Office of Inspector General (OIG) or contractors it hires and the U.S. Government Accountability Office (GAO).

5.6.1 Audit Types

There are several types of audits conducted at DHS that may involve ISSOs. They include Financial Statement, FISMA, IT general controls (ITGCs), and Application Controls. OMB A-123 Internal Controls reviews are also performed. While not an audit, this type of review also focuses on assessing IT general controls and is performed annually.

5.6.1.1 ITGC/Application Control Audits

A number of audits are conducted by the OIG every year. They may cover a variety of IT related topics and can be functionally oriented (e.g., access controls at a site used by multiple Components such as airports) or technology oriented (e.g., security of laptops).

5.6.1.2 Financial Statement Audits

Financial audits are conducted every year. As part of the overall financial audit, auditors also review the ITGCs of systems that store, process, or transmit financial data. Financial reviews of ITGCs are similar to Security Assessment Plans but focus on specific controls and use sampling techniques (See Section 6.2). Usually only systems on the CFO designated list are included.

5.6.1.3 FISMA Audits

The OIG conducts an annual review of the DHS Information Security Program. Every year OMB publishes a Memo with guidance for FISMA reporting and compliance (e.g., M-09-29, FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) that includes guidance for the OIG review. While the OIG is reviewing the overall DHS Security program, they test elements of individual systems at each Component as a measure of the effectiveness of the program.

5.6.1.4 OMB A-123 Internal Control Reviews

OMB A-123 Internal Control Reviews are conducted by in-house assets to determine the status of controls over financial systems. While not strictly an audit, they follow similar procedures and identify weaknesses in system controls.

5.6.2 Audit Preparation

In conducting audits, auditors perform tasks necessary to assess the controls environment and have been authorized to review and/or collect information required to perform work. The goal for ISSOs and audit liaison staff is to ensure auditors get accurate information that is as thorough

and current as possible while following normal security procedures for visit requests, clearances, connecting laptops, etc.

ISSOs should coordinate with their Component audit liaison POC to ensure the liaison is aware of the audit and the ISSO understands standard procedures for dealing with auditors at their Component. ISSOs should begin preparing for an audit as soon as notified an audit will be conducted. Before preparing for an audit, it is important to understand the audit objectives, scope, and timeframes. As appropriate within the context of the current audit, preparation should include a review of previous audits and Security Authorization Process documents to identify previous audit findings or other areas that need improvement so they can be addressed in an informed manner. As part of a compliance audit, auditors generally check implementation of controls against DHS/Component policies and procedures. Therefore, it is strongly recommended to review them and to do a preliminary internal check before auditors arrive.

ISSOs are not always directly involved in an audit, but because of their unique position and insight into an information system's security, ISSOs can provide valuable insight and should actively support audit activities. Working closely with audit liaison personnel, ISSOs should help identify people who are knowledgeable in various aspects of the audit and ensure they are briefed on audit goals, scope, and procedures and understand the procedures for interacting with auditors. DHS can provide training on how to prepare for and what to expect during an audit, if desired.

An entrance conference is held at the start of the audit or review where auditors:

- Define the audit scope and objectives (e.g., what is included/excluded, what sites will be visited, what system(s) will be assessed and the methodology for assessing them, etc.)
- Request or identify POCs
- Discuss procedures for requesting meetings, interviews, documents, etc.
- Describe the methodology that will be used (e.g., interviews, scans, etc.)

Although it may be beyond their area of responsibility, ISSOs should try to ensure key personnel who may interact with auditors attend the entrance conference.

Auditors generally collect data through document reviews, interviews, meetings, and technical testing (e.g., vulnerability scans). The following sections provide additional background and guidance in each area.

5.6.2.1 Documents

- Follow agreed on procedures when providing documents
- Ensure documents provided to auditors are what was requested and approved for release. The auditor may not know the specific name of the document and may refer to the document by the content it contains. For example, one agency may name a document the Configuration Management Plan yet another may name it Change Control Plan. However, the content of both are basically the same. The key is to

provide the auditor what was requested given that it may not be named exactly as it appears in the request

- Documents provided to auditors should be properly labeled so that the auditor is aware if they contain PII or various forms of FOUO
- In the case of GAO audits, some documents may need a legal review before being provided to the auditor. Guidance on this can be obtained from the Component audit liaison and is also contained in DHS Under Secretary for Management memo dated Sep 19, 2008

5.6.2.2 Meetings/Interviews

- Ensure the appropriate people are present to ensure the meeting is productive
- Ensure any personnel that invited are prepared for the interview
- Focus answers on the scope of the review
- Avoid trying to answer questions that are not within the audit scope
- Ask for clarification if a question is not understood
- Defer questions to the appropriate point of contact

5.6.2.3 Testing

- Rules of Engagement (ROE) or Rules of Behavior (ROB) are usually agreed upon before testing occurs. Depending on the type of audit, these may have been handled at the Department or Component management level. Rules should include POCs and a process for resolving disagreements on testing procedures
- All testing should strictly follow the ROE/ROB, if one exists
- All parties should agree on a clearly defined set of ROE or ROB before testing starts. Rules should include POCs and a process for resolving disagreements on testing procedures
- Sensitive data and system availability should be protected at appropriate levels during all stages of the audit

5.7 Auditing (Logging) and Analysis

The purpose of auditing system activity is to capture sufficient information in audit logs to establish what events occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.

Auditing supports accountability by providing a trail of user actions. For this reason, it is important to be able to tie individual users to each action. This is one reason that using shared or group passwords is not allowed.

⚠ **Always ask for clarification whenever anything is not clear.** Auditors sometimes use terminology that is not familiar to the person being audited but should provide clarification when asked.

Because the audit trail is used to ensure accountability, both the audit data itself and the mechanisms to determine what audit data is recorded must be protected from unauthorized access, modification, or destruction. In addition, audit trail data must be available in an easily readable form and in a timely manner and should be reviewed periodically to discover security violations, identify undesirable trends, and provide assurance that security controls are working as intended and users are following proper procedures. In some cases, audit data can reveal the need for increased user or operator training, identify necessary changes or improvements to procedures, or suggest ways to strengthen system or application performance, even if no security violation occurred.

5.7.1 Audit Events

The following events should always be logged*:*

- Logon/off, both to the system and to the application
- Failed authentication attempts
- Resource access attempts that are denied by the access control mechanism
- Privileged user actions
- Activities that require privilege
- All attempted accesses of security related resources, whether successful or not
- Creation or deletion of users
- Changes to user security information or access rights
- Changes to system security configuration
- Changes to system software
- Attempts at escalation of privileges

For each recorded event, the audit record should identify, at a minimum:

- Date and time of the event
- User ID and associated point of physical access (e.g., terminal, port, network address or communication device)
- Type of event
- Names of resources accessed
- Success or failure of the event

5.7.2 Audit Log Review

The ISSO should ensure audit logs are reviewed at least weekly, but more frequently if resources permit. When reviewing logs, some events will require follow-up inquiries to determine if a problem exists, whether corrective action is required, or if there is another explanation for

unusual activity. The following are examples of the type of activity that warrant additional attention:

- Failed logon or resource access attempts
- Unusual patterns of activity (e.g., users who suddenly begin to log in after normal working hours)

⚠ User passwords should never be recorded in logs.

- Changes to existing patterns of activity (e.g., authorized users performing authorized functions they do not normally perform)
- Unusual or increased activity by privileged users
- Any unexpected or unexplained changes to system security settings
- Normal activities under unusual circumstances (e.g., logon by a user known to be on vacation or the same user logged on from different physical locations simultaneously)
- Activities indicating users are sharing or otherwise misusing passwords
- User anomalies (e.g., a user who is locked out more than other users, a user who needs significantly more help desk support than other users, a user who continually forgets his/her password)
- System reboots at unusual times or an increase in the number of system reboots
- Any significant changes in normal patterns

5.7.3 Audit Log Retention and Storage

Audit logs must be available online for at least 90 days and must be retained off-line for at least 7 years.

To ensure storage limitations do not impact auditing retention requirements, ISSOs should determine the amount of storage required to store a normal number of logs for 90 days on the system for each security relevant system element. Then the ISSO should allocate at least 120% of the usual log size for 90 days' worth of logs for that device either on the local device or on a centralized logging server. The ISSO should configure each device and/or the centralized server to alert the SA in the event that the log storage area reaches or exceeds 90% of allocated size. ISSOs or system administrators should perform a manual review of available audit storage space to ensure log files have not exceeded their allocated space at least quarterly.

5.8 Budget

ISSOs should make their SOs and program managers aware of high cost items that will be needed in sufficient time to ensure there is funding for them. Because each organization may have a different budget timeline, ISSOs should coordinate with their SOs early in the year to ensure they can provide input before budgets are submitted. Items that may need to be funded separately include things like the Security Authorization Process, new equipment or licenses (e.g., firewalls), scans or scanning tools, training, and, occasionally, remediation efforts for

POA&Ms. The goal in this area is to ensure the SO or program manager is aware of upcoming expenses in time to consider how they will be funded.

5.9 Security Authorization Process

All systems must have a valid Authority to Operate (ATO) through the Security Authorization Process.. If a system is not in Ongoing Authorization, it must be re-authorized before the ATO expires. Systems in Ongoing Authorization may need to be re-authorized if the system is removed from Ongoing Authorization. Additionally, systems may need to be re-authorized if significant changes occur that could affect the risk posture of the system. Significant changes include such things as re-hosting the system to a new facility, upgrading or changing the operating system, making changes to system functionality, or a change in the system's security posture.

In some cases, Components may use a Type Accreditation for information resources that are under the same direct management control; have the same function or mission objective, operating characteristics, security needs, and that reside in the same general operating environment, or in the case of a distributed system, reside in various locations with similar operating environments. A Type Accreditation is appropriate for a general support system deployed at multiple sites but operating in a specified environment. For example, several organizations within DHS provide services over large distributed environments (e.g., field sites at airports and border crossings). These field sites are equipped with remote network connections, client-server solutions, and other resources, all of which must be authorized for operation and accounted for in DHS IT security risk analyses and FISMA reports. The cost to independently evaluate and authorize each of these sites is prohibitive. A Type Accreditation, however, allows for common security controls across the sites to be consolidated and for a single master Security Authorization Process to be conducted. To account for unique physical and logical variations at the site level, a description of any differences and the associated risks at each site are documented, and the site-specific documents are incorporated as attachments or appendices to the master Security Authorization Package. A Type Accreditation consists of a master Security Authorization Package describing the common controls implemented across sites and site-specific controls and unique requirements that have been implemented at the individual sites. DHS 4300A, Attachment D, Type Accreditation, provides specific guidance on Type Accreditation.

ISSOs are not always directly responsible for conducting Security Authorization Processes but need to monitor and oversee the process. ISSOs need to be aware of the status and expiration of the ATO. All systems must have a valid ATO prior to becoming operational. Systems not under OA must be re-authorized every three years (or earlier as determined by the AO) or when significant changes occur. The ISSO should initiate action early enough to ensure the Security Authorization Process is completed before the system becomes operational or the current ATO expires. This will entail working closely with the SO or program manager to ensure resources are available to both conduct and to participate in the Security Authorization Process. Regardless of how the process is implemented, the ISSO should take the lead to ensure documents are submitted to the SCA and available in the IACS tool for DHS validation. ISSOs should coordinate closely with the SCA and the AO before and during the Security Authorization

Process to ensure they are aware of requirements, processes and expectations. ISSOs should be thoroughly familiar with the DR process and checklists at the start of the Security Authorization Process to ensure a compliant package is developed. See Section 2.1.1 for additional information on the document review process.

Figure 3. ISSO Security Authorization Process Relationships illustrates the primary POCs the ISSO will interact with during the Security Authorization Process with arrows depicting the flow of information and documentation.

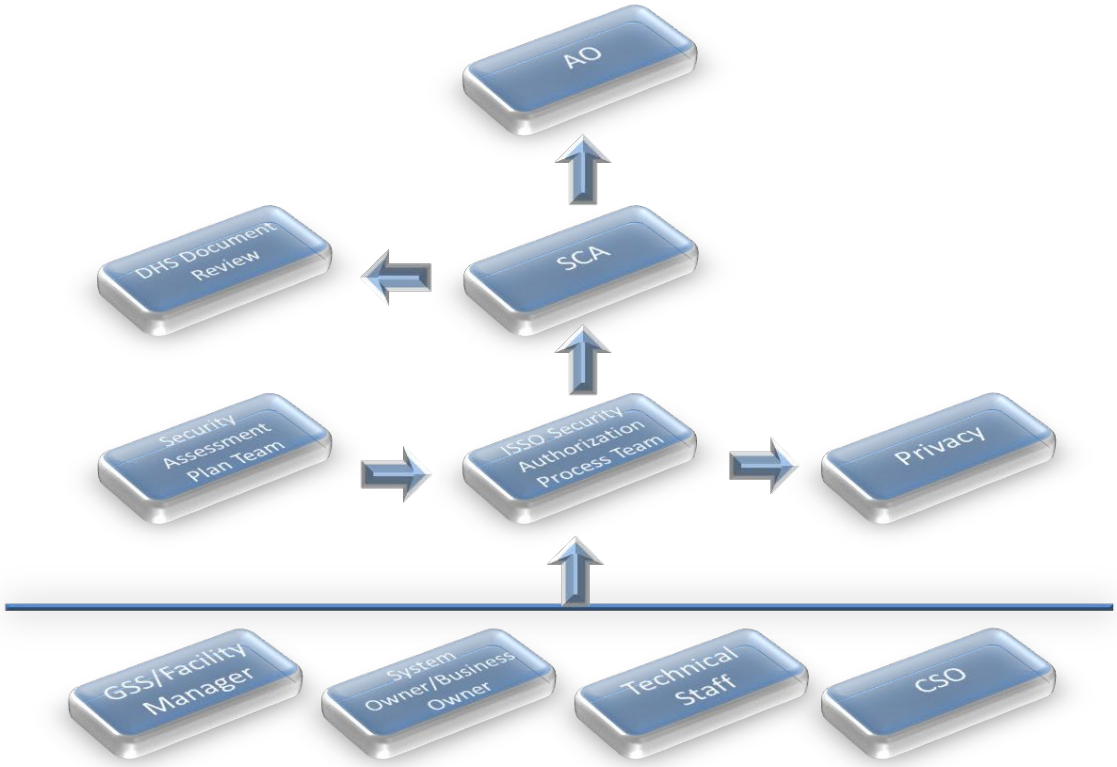

Figure 3. ISSO Security Authorization Process Relationships

The DHS Security Authorization Process is described in detail in the DHS Security Authorization Process Guide. A list of documents required for a fully compliant Security Authorization Package is provided in the annual Performance Plan. Steps for conducting an initial Security Authorization and a re-authorization are essentially the same. The primary difference is that an initial ATO should be started early in the SELC process while re-authorization will usually begin 4-6 months before the current ATO expires. The 4-6 month timeframe assumes that resources are available to start the Security Authorization Process. Additional lead time may be needed for contracting or otherwise obtaining the Security Authorization Process team. Systems implementing OA do not require re-authorization unless they are removed from the OA program.

AOs may grant an IATO for systems that are undergoing development testing or are in a prototype phase of development. A system must be accredited and authorized in an ATO letter prior to passing the Key Decision Point 3 milestone in the development life cycle. The AO may grant an IATO for a maximum period of six months and may grant one extension for up to six months. IATOs are not allowed for operational systems.

5.10 Common Controls

Common controls are security controls whose implementation results in a security capability that is inheritable by one or more organizational information systems. Security controls are deemed inheritable by information systems or information system components when the systems or components receive protection from the implemented controls but the controls are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the systems or components—entities internal or external to the organizations where the systems or components reside. Security capabilities provided by common controls can be inherited from many sources including, for example, organizations, organizational mission/business lines, sites, enclaves, environments of operation, or other information systems. Many of the controls needed to protect organizational information systems (e.g., security awareness training, incident response plans, physical access to facilities, rules of behavior) are excellent candidates for common control status. In addition, there can also be a variety of technology-based common controls (e.g., Public Key Infrastructure (PKI), authorized secure standard configurations for clients/servers, access control systems, boundary protection, cross-domain solutions). By centrally managing and documenting the development, implementation, assessment, authorization, and monitoring of common controls, security costs can be amortized across multiple information systems.

Regardless of whether they are common, ISSOs are still responsible for documenting and ensuring all applicable controls are implemented effectively. Outsourcing the implementation of a control does not mean it is effective or satisfies system requirements. Common controls that are hybrid (partially inherited) must have additional implementation steps in the system security plan to ensure it satisfies the security control.

NIST Special Publication (SP) 800-37 allows agencies to centrally manage common security controls in a dispersed environment. Attributes for common security controls include:

- Common security controls can apply to an information system, subsystem, or application (i.e., common hardware, software, and/or firmware) deployed at multiple operational sites.
- The development, implementation, and assessment of common security controls can be assigned to responsible officials other than the information SOs whose systems will implement or use those common security controls.

The results from the assessment of the common security controls can be used to support a Type Security Authorization. The process shall consist of a master Security Authorization Package describing the common controls implemented across sites and site-specific controls and unique requirements implemented at the individual sites.

5.11 Configuration Management (CM)

As new systems and newly modified systems proceed through the SELC, changes must be documented and tested prior to placing the systems into the operational environment. This includes testing of security controls. The objective is to ensure new vulnerabilities are not introduced during the change process. The same requirements apply to operational systems as they undergo periodic modifications. Changes must be documented and tested prior to placing the system back into the operational environment. CM begins with base-line requirements documentation and ends with decommissioning of items no longer used for production or support. CM must be applied to hardware, software, firmware, documentation, test and support equipment, and spares.

The ISSO and Project Manager work with the appropriate development team (for new development systems) or the Operations and Maintenance (O&M) Support Team (for fielded systems) to ensure all proposed changes to the configuration baseline are analyzed and tested to determine their security implications. As new vulnerabilities are identified during the testing process, appropriate security software patches must be tested and installed prior to implementation of the proposed change. Any changes that impact the security posture of the system must be brought to the attention of the SCA and the AO.

Specific ISSO Configuration Management responsibilities include:

- Ensure all proposed configuration changes are analyzed prior to implementation to determine if the proposed change has security implications
- Ensure all proposed configuration changes to operating systems, operating system security features, applications, critical system files, and system devices are formally approved, tested, and documented prior to the change being implemented
- Ensure accurate system documentation and configuration logs are maintained to reflect current and prior configuration baselines
- Ensure the configuration of subordinate IT system elements is consistent with the Security Authorization Process requirements of the parent system
- Ensure a current, baseline configuration of the system and an inventory of its components are developed, documented, and maintained
- Ensure security settings of information systems are set to the most restrictive mode consistent with operational requirements and DHS Sensitive Systems Configuration Guidelines
- Ensure information security patches are installed within the timeframe or direction stated within the ISVM message published by the DHS SOC
- Review the system at least annually, to identify and eliminate unnecessary functions, ports, protocols, and/or services

The DHS CISO website has a number of configuration guides for hardening system components (e.g., Cisco Routers, Oracle databases, HP-UX, ActiveDirectory, Solaris, Linux, Windows, etc.).

5.12 Contingency Planning

The purpose of the Contingency Plan (CP) and Contingency Plan Test (CPT) is to ensure the system can be recovered and the business process can continue to support the mission with the least disruption possible. Contingency planning is one of the key elements of an ISSO's responsibilities. Regardless of the requirement for a plan and tests, it is good business practice to ensure the availability of systems that supports the mission. CP tests can also be used to ensure the plan is well documented and effective and to test the organization's readiness to execute the plan.

The system contingency plan must address contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. The scope and level of detail contained in the CP is based on the security categorization for the **availability** security objective. The CP in IACS comes from Attachment K, IT Contingency Plan Template from the DHS 4300A Sensitive Systems Handbook.

After it is approved, copies of the contingency plan should be distributed to key contingency personnel and alternate storage and processing sites. Since most contingencies occur outside of normal working hours, it is important for key personnel to have access to the plan from home and alternate work sites.

DHS also requires a formal Business Impact Assessment (BIA) to be conducted and attached to the Contingency Plan. Contingency planning cannot be conducted effectively without information derived from a BIA. Among other things, a BIA will identify allowable down-time which is a key element in developing a CP.

When developing and testing the CP, it is also important to coordinate with organizational elements responsible for related but separate plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, and Incident Response Plan).

ISSOs are also required to ensure personnel are trained in their contingency roles and responsibilities. Wherever possible, simulated events should be incorporated into contingency training to facilitate effective response by personnel in crisis situations. For this reason, the best training will occur when the plan is actually being tested.

The CP for all systems must be tested **at least annually** by the anniversary of the ATO and results uploaded in the IACS tool. A tabletop test is all that is required for low availability systems but it is still a good idea to test restoration from backups. For moderate and high availability systems testing must be conducted in the following phases: Activation and Relocation (0 to 12 hours), Alternate Facility Operations (12 hours to termination), and Reconstitution (termination and return to normal operations).

Types of tests that should be conducted include:

- POC updates should verify all phone numbers listed in the plan, to include various team members, alternate storage and processing sites and vendors. The tester should actually dial the numbers to see who answers and ensure people assigned CP roles are still in their position. For vendors, the tester should also verify account numbers and

contract numbers / status. Although this test is only **required annually**, it should be conducted every three to six months because people tend to change jobs or locations and it is a relatively easy test to conduct

- Tabletop exercises should include all personnel who play a key role in executing the plan. All systems should conduct tabletop exercises, even if a full recovery at an alternate site is planned. The tabletop exercise may point out potential problems that can be resolved before a more expensive / extensive recovery exercise is conducted. Tabletop exercises can also be used as a means of training people with key CP responsibilities. The tabletop exercise should walk through the plan with all stakeholders to ensure:
    - There are no obvious gaps or inconsistencies in the plan (e.g., the same key person does not have to be at the disaster site and alternate site at the same time)
    - Key roles have been assigned to people who are capable of carrying them out (i.e., they have the technical competence and organizational authority to carry them out)
    - Timelines are realistic and consistent with contracts and Service Level Agreements (SLAs) (e.g., the offsite storage vendor's contract states backups need to be available within 24 hours but the CP states the system must be restored in six hours)
    - Prioritization and recovery sequence are consistent and clearly described;
    - Essential people know their responsibilities and dependencies on other people and tasks
    - Essential people know where they should report in an emergency and they know how to get there (e.g., where exactly is that alternate site?)
- Restoration from backups should be conducted every three to six months but must be conducted at least annually for moderate and high availability systems. Backups should include full data backups on a weekly basis, with incremental data backups on a daily basis. System and application software must be backed up for all high availability systems whenever modifications are made to the software. This is a good practice for moderate and low availability systems as well. The purpose of testing backups is to ensure:
    - Backups can be retrieved from the off-site storage facility within required timelines
    - Restoration procedures can be implemented by available staff and are effective
    - Data and media have not been corrupted
- Tests of the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations

ISSOs should visit alternate processing (and storage) sites to confirm:

- Physical and environment controls are adequate
- The alternate processing site is fully configured to support a minimum required operational capability and ready to use as an operational site
- Alternate processing site agreements contain priority-of-service provisions in accordance with the organization's availability requirements
- The alternate site is geographically separated from the primary storage site so as not to be susceptible to the same hazards. The primary and alternate sites should be physically separated by at least 50 miles

5.13 Continuous Monitoring

Continuous Monitoring entails all activities conducted to ensure security controls remain effective over time. Specific continuous monitoring activities include:

- Annual assessments
- Audit log reviews
- Documentation updates
- Vulnerability scanning
- Account maintenance
- Review of access lists
- Third party compliance monitoring
- Training
- Incident response testing
- Configuration management
- System element inventory
- Key/combination/badge maintenance
- Risk designations
- Physical access monitoring
- ISVMs/patching

Appendix C contains a list of DHS OIG approved security testing tools and utilities that can be used in a testing program.

To assess the continuous monitoring process, DHS has implemented an annual performance plan that reviews specified security metrics and reports them through use of a monthly scorecard. While the scorecard is published monthly and distributed to the CIO Council and CISO Council,

it is available to Components via Crystal Reports on a daily basis. ISSOs should be thoroughly familiar with the annual Performance Plan.

5.14 Identification and Authentication

ISSO responsibilities regarding Identification and Authentication include ensuring there are procedures to:

- Authorize and issue user identifier
- Ensure the user identifier is issued to the intended party
- Disable user identifier after 45 days of inactivity

5.15 Incident Response including PII

Most Incident Response requirements are implemented by DHS or Component Computer Emergency Response Team (CERT)/SOCs. ISSO responsibilities regarding incident response include:

- Ensure system operations personnel and users are trained in the proper procedures for recognizing and reporting security incidents
- Ensure system development and site personnel submit incident reports as required
- Provide input to weekly incident response reports
- Receive ISVM messages and report compliance
- Track and document information system security incidents on an ongoing basis

For incidents involving Privacy information, the ISSO must ensure the Privacy Officer is informed in a timely manner in accordance with Component-specific guidance.

It is important for the ISSO be familiar with incident response procedures and the types of incident that are reportable vs. non-reportable.

Incident reporting should follow Component Specific Procedures within the following DHS Guidelines:

- Significant incidents must be reported to the DHS SOC by calling (703) 921-6505 as soon as possible but not later than one hour from "validation" (e.g. a security event being confirmed as a security incident). Other means, such as the SOC ONLINE portal are acceptable, but the Component shall positively verify the notification is received and acknowledged by the DHS SOC
- Minor incidents on systems may be reported in the weekly incident report. SBU systems may report via the DHS SOC portal . Components with no portal access shall report minor incidents via email. HSDN incidents or incidents involving SECRET information shall be documented in a summary report via the HSDN DHS SOC

5.16 Interconnection Security Agreements and Memoranda of Understanding / Agreement

An Interconnection Security Agreement (ISA) is used to specify the technical and security requirements for connecting two systems while an Memoranda of Understanding / Agreement (MOU/MOA) defines the responsibilities of the participating organizations. ISAs are intended to ensure that both systems protect sensitive data at the same level and have implemented appropriate security controls. As an ISSO, it is important that ISAs are in place to ensure that your system and data are protected once it is shared with another system or organization.

An ISA is required whenever the security categorization levels are not the same or there is a different AO for each system. ISSO responsibilities regarding ISAs include:

- Ensure all external connections are documented in the SP and security operating procedures
- Determine if an ISA is needed – not all connections require an ISA
- Coordinate with external organization to develop the ISA
- Assist in preparation of the ISA
- Review ISAs as a part of the annual FISMA self-assessment
- Monitor compliance

In practice, ISSOs may actually collect data and draft ISAs or MOU/MOAs that are needed. The AOs must sign the ISA before the associated connection becomes operational.ISAs must be re-issued whenever a re-accreditation is required. ISSOs must review ISAs as part of the annual FISMA self-assessment.

The ISA documents requirements for connecting the IT systems, describes the security controls that will be used to protect the systems and data, contains a topological drawing of the interconnection, and provides a signature line. The ISA includes descriptive, technical, procedural, and planning information. It also formalizes the security understanding between the authorities responsible for the electronic connection between the systems. The ISA also supports a MOU/A between the organizations.

The MOU/A documents the terms and conditions for sharing data and information resources in a secure manner. Specifically, the MOU/A:

- Defines the purpose of the interconnection
- Identifies relevant authorities
- Specifies the responsibilities of both organizations
- Defines the terms of agreement, including sharing costs and the timeline for terminating or reauthorizing the interconnection

This brief nontechnical agreement is the authorization for detailed planning of an interconnection, leading to an ISA. The MOU/A should not include technical details on how the interconnection is established or maintained; that is the function of the ISA.

5.17 Inventory

The information system inventory is the foundation for all information security activities. The DHS FISMA inventory is the official record of systems within DHS and is used as the basis of FISMA reporting to Congress and OMB as well as for computing the monthly FISMA scorecard. The FISMA Inventory establishes a common baseline for tracking systems as part of the Enterprise Architecture Board (EAB), Budget Requests, Information Technology Acquisition Reviews (ITAR), and Data Center Interim Change Control Board. The DHS FISMA inventory is also used to support information resources management; IT planning, budgeting, and acquisition; the monitoring, testing, and evaluation of information security controls; and the preparation of the index of major information systems required pursuant to the Freedom of Information Act (FOIA).

All updates to the inventory must be requested through submission of Change Requests (CRs). Inventory change requests should be submitted every time the life cycle stage changes (e.g., development to operational) or when major system changes occur that require re-authorization.

Systems should be entered in the database beginning with the initiation phase and updated accordingly through disposal. Change requests should be submitted within 30 days of a change. Change requests can only be submitted by the Component CISO but are usually initiated by the ISSO who has a profound understanding of the system status. CR forms and submission procedures are available in the DHS FISMA System Inventory Methodology.

The DHS FISMA System Inventory Methodology also provides guidance on how to determine system boundaries. In general, each element of the system must:

- Be an interconnected set of resources under the *same* direct management control
- Have the *same* function or mission objective
- Have essentially the *same* operating characteristics and security needs
- Reside in the *same* general operating environment or, in the case of a distributed information system (e.g. type accreditation situations), reside in various locations with common operating environments (COE) and security controls

The final factor to determine system boundaries is budgetary control. If the elements receive funding from the same source, they can be regarded as having the same direct management control. If they are funded by disparate sources, they should be considered as having different management control and recorded in the inventory as separate systems.

All IT assets must be included in the inventory as part of a system in one of the following system categories (*denotes system subcategories):

- Major Application (**MAJ)**
- General Support System (**GSS)**
- Type Security Authorized System* (**TYP)**
- Minor Application* (**MIN)**

- Subsystem*** (SUB)**

ISSOs should ensure that data in the FISMA inventory database, IACS, and the SP are current and consistent.

Questions regarding inventory issues can be addressed to the DHS Inventory Team at:

fisma.inventory@dhs.gov.

5.18 Maintenance

System maintenance involves performing and documenting routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. ISSO responsibilities in this area include ensuring all media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) is scanned for malicious code before the media is used and all maintenance equipment with the capability of retaining information is appropriately sanitized before release.

5.19 Media Protection

ISSO must ensure procedures are in place and followed such that:

- Only authorized users have access to information in printed form or on digital media
- The pickup, receipt, transfer, and delivery of such media is restricted to authorized personnel
- All system output, whether paper or electronic, have external labels indicating the distribution limitations and handling caveats of the information
- System digital media is properly sanitized or destroyed, using approved equipment, techniques, and procedures, before its disposal or release for reuse
- Media sanitization actions are tracked, documented, and verified and that sanitization equipment/procedures are tested periodically to ensure correct performance

5.20 Patch Management

The SOC issues ISVM messages whenever a new vulnerability is discovered and a patch is issued. ISSOs should ensure they are on distribution for these messages (e-mails).

When an ISVM is received, ISSOs should check with the technical lead (or may already know) to determine if the patch applies to their system and, if so, when it will be installed. The ISSO should acknowledge receipt of the ISVM and report compliance or notify the granting of waivers within the timeframes specified. ISSOs should check local requirements since some Components have ISSOs report to a central POC rather than the SOC. A sample ISVM outline is provided below:

CSIRC ISVM Number:

CVE Number:

Topic:

Priority: High / Moderate / Low

Acknowledgement Required: Yes / No

Acknowledgement Due Date:

Compliance Response Required: Yes / No

Compliance Due Date:

Release Date:

Revision Summary:

Software Affected:

Overview:

Action:

Description:

ISSOs should validate that all patches have been successfully applied within the specified timeframe and also periodically review the status of these patches to ensure they are still in place.

5.21 Personnel Security

ISSOs generally do not have direct control over personnel security policies or procedures but are still responsible for ensuring personnel controls are in place and effective. ISSOs should review policies and procedures to ensure:

- Position risk designations are reviewed and revised as needed but at least every three years
- Users are screened before being granted system access
- Termination procedures are in place to ensure accounts are deactivated when system users depart or change jobs
- Users complete appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) before being granted system access
- Reviews information systems/facilities access authorizations when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations)
- Personnel security requirements for third-party providers, whether contractors or another federal agency, are in place and effective

- A formal sanctions process for personnel failing to comply with established information security policies and procedures

5.22 Physical and Environmental Security

Physical and Environmental Security controls are intended to deter, detect, restrict, and regulate access to sensitive areas to safeguard against possible compromise, loss, theft, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters. The following sections discuss key elements of both physical and environmental controls, as well as the need to provide for the safety of people who use or operate systems.

5.22.1 Physical Security

Information systems must be physically protected to prevent unauthorized disclosure, denial of service, theft, destruction, or modification. Physical security represents the first line of defense against intruders attempting to gain physical access to systems and must be addressed during each step of the risk management cycle.

Facility Managers are responsible for ensuring physical and environmental controls are in place and working properly at all times. ISSOs are responsible for working with Site Security Officers to ensure:

- Access is restricted only to authorized individuals, and there is a process for approving /removing access. Access lists are reviewed and re-approved at least annually
- An effective process has been implemented to provide oversight of the issuing and return of badges, credentials, keys, and identification documents and ensure proper reporting of their loss or theft
- Badges should be displayed above the waist and below the neck with the photo side facing out
- Offices are inspected periodically, during or after working hours, to ensure that sensitive and proprietary materials are being adequately safeguarded
- Third party providers and contractors comply with applicable security regulations environment
- Government-owned and controlled property, funds, and valuables are properly safeguarded and accounted for
- Physical security risks are reviewed and evaluated throughout the SELC
- Effective procedures are in place to control visitors which include:
    - Visitor identification badges, which must be turned in upon leaving the facility
    - Visitor escorts in areas that contain sensitive information
    - A visitor access log that includes:

        - Name and organization of the person visiting
        - Signature of the visitor
        - Form of identification
        - Date of access
        - Time of entry and departure
        - Purpose of visit
        - Name and organization of person visited
    - Retention of visitor logs for one year
- Physical access to information system transmission lines carrying unencrypted information is controlled to prevent eavesdropping, in-transit modification, disruption, or physical tampering
- System-related items (i.e., hardware, firmware, software) entering and exiting the facility are controlled and appropriate records of those items are maintained. Property passes should be used for personal equipment entering and leaving the facility

5.22.2 Environmental Controls

Environmental controls are intended to protect systems against threats associated with power, fire, water, heat and humidity, and other natural causes.

ISSOs must ensure environmental controls are in place and functioning properly, even if their system is hosted at a third-party site, and the system Contingency Plan provides a means to restore environmental conditions to allow continued system operations. The following sections describe ISSO guidance in each of these areas.

5.22.2.1 Fire Protection

Fire protection systems should be serviced by professionals on a recurring basis to ensure the system stays in proper working order.

When a centralized fire suppression system is not in use, fire extinguishers must be readily available. Facilities should use Class C fire extinguishers (which are designed for use with electrical fire and other types of fire). Fire extinguishers should be located in such a way that a user would not need to travel more than 50 feet to retrieve it. Fire extinguishers should be tested at least annually (check the tag on each extinguisher).

Fire drills must be conducted annually to ensure all personnel are familiar with their responsibilities.

5.22.2.2 Water

Means to protect against water damage resulting from broken plumbing lines or other sources of water leakage, such as fire system activation, must be in place or readily available, to include accessible master shutoff valves that are accessible, working properly, and known to key personnel.

5.22.2.3 Power Supply Protection

Electrical power must be filtered through an uninterruptible power supply (UPS) system for all servers and critical workstations and surge suppressing power strips used to protect all other computer equipment from power surges. UPS capabilities provide enough time to activate alternate power sources or allow a graceful system shut down.

5.22.2.4 Temperature and Humidity Control

Temperatures in computer storage areas should be held between 60 and 70 degrees Fahrenheit. Humidity should be at a level between 35 percent and 65 percent. Most systems will continue to function when temperatures and humidity go beyond this range, but the associated risk to data is increased. Low humidity can result in static and high temperature can damage sensitive components of computer systems.

A device that will sound an alarm and send out an automatic notification (via email or pager) when the operating environment exceeds recommended boundaries should be used in computer rooms.

5.22.2.5 Housekeeping Considerations

Housekeeping is another important area to monitor to help protect IT equipment from damage. Dusting of hardware and vacuuming of work areas should be performed weekly with trash removal performed daily. Dust accumulation inside of monitors and computers is a hazard that can damage computer hardware. Cleaning supplies should not be stored inside the computer room. Sub-floors (where installed) should be cleaned annually.

5.22.3 Personnel Safety Features

Personnel Safety is the primary consideration when determining and maintaining physical and environmental controls. ISSOs should ensure emergency exits and emergency equipment, such as fire extinguishers and first-aid kits, are clearly marked and easily accessible. Emergency power and water shut off mechanisms should also be clearly marked and easily accessible.

5.23 Planning

Discussions of planning in the security environment usually revolve around the SP.

The SP is a living document that should be updated whenever there are changes to the system but at least annually. The most common changes to the SP result from personnel changes (e.g., ISSO, SO, etc.). The current version of the SP should be uploaded into IACS.

- The SELC requires the ISSO to be involved in planning from the earliest phases for developing requirements and ensuring they are included in the design
- Planning for re-accreditation activities is a critical part of ISSO responsibilities. ISSOs must be aware of the current ATO expiration date and initiate action to conduct a Security Authorization Process in enough time to ensure it is complete prior to expiration

- Planning to resolve system weaknesses is a critical ISSO responsibility, involving development of POA&Ms whenever a weakness has been identified

5.24 POA&M Management

ISSOs are responsible for documenting POA&Ms in IACS. ISSOs also are tasked with developing POA&Ms for all identified weaknesses. However, ISSOs cannot create POA&Ms without significant input and buy-in from program managers, SOs, technical staff and possibly others. When weaknesses are identified, ISSOs should schedule a meeting with stakeholders to develop milestones, identify and allocate resources and determine the remediation schedule.

When planning POA&M completion dates, it is best to select a scheduled completion date in the middle of the month rather than the last day, if possible. This allows some leeway for updating the POA&M status if there is a delay to help remain green on the scorecard, which is based on data pulled on the first day of the month.

Once POA&Ms have been created and documented, ISSOs can manage the POA&M process by reviewing daily detail reports from Crystal Reports or using the Weakness Search Report Guide (See Appendix G of the POA&M Guide). It is a good practice for ISSOs review weekly, but at least monthly, to determine POA&Ms that are scheduled for completion in the near term and check the status with responsible parties. DHS 4300A Attachment H, POA&M Guide provides detailed guidance regarding the POA&M process and documenting POA&Ms.

5.25 Risk Assessment

Risk assessment is an ongoing ISSO responsibility throughout the SELC. Formal Risk Assessments are conducted as part of the Security Authorization Process. Additionally, informal risk assessments should be conducted as part of the annual assessment process, following any automated scans, and whenever ISVMs are issued.Rules of Behavior

ROB documents provide all users information about their information system responsibilities. ROB ensure information system users acknowledge that they understand what is expected and that they will be held accountable for their actions when processing, storing, and handling DHS information. ROB must be developed for each system. They must clearly delineate responsibilities and the expected behavior of all individuals, and must state the consequences of noncompliance. ISSOs should ensure that ROBs are signed by all system users before they are granted system access. DHS 4300A, Attachment G: Rules of Behavior provides sample rules that are applicable to all systems and should serve as a starting point for ISSOs to develop system specific ROB. ROB should include guidelines for privileged users (e.g., system administrator, DBA, etc.) as well as end users.

5.26 System and Communications Protection

ISSO responsibilities in this area include ensuring:

- Any cryptographic mechanisms used by the system are FIPS 140-2 compliant

- Publicly accessible system components (e.g., public web servers) are on separate sub-networks with separate, physical network interfaces
- The public cannot gain access into the organization's internal networks except as appropriately mediated
- The system separates user functionality from information system management functionality and isolates security functions from non-security functions

5.27 System and Information Integrity

ISSO responsibilities regarding System and Information Integrity involve ensuring that appropriate controls are in place. These include:

- Virus, spam, and spyware protection are in place and kept current
- The system is protected by firewalls/Intrusion Detection Systems (IDS) as appropriate
- ISVMs are sent to appropriate personnel and appropriate actions are taken in response

5.28 System and Services Acquisition

Section 5.3 Acquisition Process provides an overview of the acquisition process. This section provides guidance for ISSO responsibilities regarding System and Services Acquisition.

ISSO responsibilities during the acquisition process include, but are not limited to ensuring:

- Contracts include appropriate security requirements and/or security specifications
- The vendor provides documentation describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components)
- The vendor provides documentation describing the functional properties of the security controls employed within the information system in sufficient detail to permit analysis and testing of the controls
- The system has secure development and test environments that will not compromise system security features or operational data, and downloading and installation of unlicensed or unauthorized software is prohibited
- The system developer creates and implements a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation
- Systems under development are entered in the FISMA inventory not later than the Development Phase of the SELC
- Systems have a valid ATO before they begin to process operational data

5.29 System Interconnections

NIST defines a system interconnection as the direct connection of two or more IT systems for the purpose of sharing data and other information resources. To put it more simply, a system interconnection is defined as any time data crosses the Security Authorization Process boundary. All system interconnections need to be identified and documented in the SP, whether or not they require an ISA. It is important for ISSOs to know and understand data flow within and outside their systems to ensure proper protections are in place and that their data is safe during transmission and receipt by another system. See Section 5.16 for information about ISAs. See NIST Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Technology Systems* for additional information in system interconnections.

5.30 Security Training

Annual Security Awareness and Training is addressed in Section 5.5. This section provides additional guidance of particular interest to ISSOs.

5.30.1 ISSO Training

ISSOs should check with their CISO office to determine what training is available. Most Components have training opportunities for ISSOs on a weekly, quarterly, or periodic basis. Some Components also have formal training opportunities such as annual conferences or week-long training courses.

Training is also available from DHS on request, through the DHS InfoSec Customer Service Center, on the following topics:

- IACS
- Annual Performance Plan
- FISMA Scorecard
- Security Authorization Process Document Review
- POA&M Process
- POA&Ms for Financial Systems
- Root Cause Analysis for POA&Ms
- Preparing for Audits
- Ad hoc training and assist visits tailored to a specific need

All requests for training should be made through the Component CISO.

6.0 REQUIREMENTS FOR PRIVACY SYSTEMS AND CFO DESIGNATED SYSTEMS

Privacy Systems and CFO Designated Systems are subject to the same requirements as all systems within DHS. However, they have additional controls that must also be met as described below.

6.1 Privacy Systems

The Chief Privacy Officer designates Privacy Sensitive Systems based on validated Privacy Threshold Analyses (PTA). Privacy Sensitive Systems are those that maintain Personally Identifiable Information (PII).

ISSOs for Privacy Sensitive Systems should be aware of the following additional requirements for their systems.

- Privacy systems must be at least a **"moderate"** for confidentiality
- As part of the Security Authorization Process, PTAs are sent to the Component Privacy office via Component-specific procedures. PTAs are subsequently sent to, reviewed, and approved by the DHS Privacy Office, not the OCISO. The OCISO approves / validates all other documents. The Privacy Office makes the determination regarding whether a system is a Privacy Sensitive System and whether a Privacy Impact Assessment (PIA) or System of Records Notice (SORN) is required. Inquiries regarding the status of a PTA should be directed to pia@dhs.gov
- ISSOs must ensure the Chief Privacy Officer or PPOC is informed expeditiously of all incidents involving Privacy Sensitive Systems because the Chief Privacy Officer is responsible for oversight of all privacy incident management
- When conducting an annual assessment of privacy systems, ISSOs must complete all of the key controls for privacy systems as well as the standard key controls. All key controls for privacy systems may be counted in the one third of controls that need to be reviewed every year.

6.2 CFO Designated Systems

ISSOs should understand the distinction between CFO Designated Systems, financial systems and mixed financial systems to help ensure the systems for which they are responsible are properly classified.

CFO Designated Systems are those that store, process or transmit financial data that is material (i.e., can have a significant impact) to the DHS financial statement and therefore require additional management accountability and effective internal control. These systems can include financial systems as well as non-financial systems. The DHS CFO publishes a comprehensive list of Designated Systems during the fourth quarter of every fiscal year. The list is reviewed and updated (if needed) annually by the DHS CFO and distributed to Component CFOs, CIOs, and CISOs. It may change from year to year depending on a number of factors. It is incumbent on

ISSOs to know whether their system is on this list. CFO Designated Systems are identified every year by the DHS Inventory Team.

All CFO Designated Systems must be assigned a minimum impact level of "**moderate**" for confidentiality, integrity, and availability. If warranted by a risk based assessment, the integrity objective should be elevated to "**high**."

Financial systems include those that have a primary function to store or process financial data. This includes any system which is used for any of the following:

- Collecting, processing, maintaining, transmitting, and reporting data about financial events
- Supporting financial planning or budgeting activities
- Accumulating and reporting cost information
- Supporting the preparation of financial statements

Financial systems are not necessarily on the CFO designated list, depending on their relevance to the overall impact on the financial statement.

Mixed financial systems are those that support both financial and non-financial functions. Mixed financial systems may or may not be on the CFO designated list.

ISSOs of CFO Designated Systems have the same duties and responsibilities as all ISSOs with two major differences, assessments and audits, as described below.

6.2.1 Annual Assessments

When conducting an assessment of CFO Designated Systems, ISSOs must complete all of the key controls for CFO Designated Systems as well as the standard key controls. All key controls for CFO Designated Systems may be counted in the one third of controls that need to be reviewed every year.

The key controls for CFO Designated Systems are identified in the DHS 4300A Sensitive Systems Handbook, Attachment R: Compliance Framework for CFO Designated Systems. In addition, the DHS CISO tri-fold identifies the NIST Special Publication (SP) 800-53 controls that have been designated for CFO systems but does not include the relevant controls from the DHS Sensitive Systems Handbook.

6.2.2 Audits

Every year, DHS and all Components must "balance their books" and issue a financial statement that includes a level of confidence that the statement is accurate. Every year, the financial statement is audited under the auspices of the DHS OIG to ensure an independent review is conducted. The audit includes a review of ITGCs of select DHS systems. Within the context of this document, ITGCs are similar to NIST Special Publication (SP) 800-53 controls that apply to financial systems.

ISSOs for the systems included in the scope of the audit should be prepared to be involved in the audit. DHS OCISO can provide training to help prepare and respond to these audits and assist the Component with the audit to a limited extent. DHS OCISO has assigned an audit liaison to

each Component, and ISSOs should know their Component audit Liaison and use them as a resource, as needed.

6.2.2.1 Test of Design (TOD) and Test of Effectiveness (TOE)

Financial audits and A-123 reviews use two terms that may not be familiar to the average ISSO. They are: Test of Design (TOD) and Test of Effectiveness (TOE).

A TOD is intended to ensure there are documented processes and procedures are in place for implementing ITGCs (i.e., controls). TOD does not refer to system design, but rather to the design of controls. A TOD generally includes reviews of policies and procedures.

A TOE is intended to ensure the controls are implemented as designed and are effective in meeting the control objective. This part of the review most closely resembles a Security Assessment Plan. However, one major difference is that financial auditors are trying to ensure that controls have been in place and operating effectively over a period of time, unlike a typical Security Assessment Plan which captures a "snapshot in time." Typically, controls that have not been implemented for more than six to nine months, sometimes longer, will fail the audit. Additionally, financial auditors use sampling methods based on established financial auditing standards. The sample size may appear to be quite small to information security professionals but it is a valid measure of effectiveness. For example, auditors may review 100 access control authorization forms against a user list to ensure users are properly authorized and fail the system if only one or two are missing.

6.2.2.2 Notice of Findings and Recommendations (NFRs)

NFRs are issued to document weaknesses that were discovered during the audit. Draft NFRs are usually sent to Components for review and comment prior to being formally issued. ISSOs should review draft NFRs to ensure they are factually accurate and the recommendations address the findings. In some cases, auditors may be willing to negotiate language in NFRs to clarify or help better define the finding or recommendation to remediate the weakness.

Note that simply implementing the recommendation may not resolve the weakness identified in the IT NFR. ISSOs and SOs need to review the findings and recommendations and conduct a root cause analysis to ensure the correct remediation action is being taken to close the finding.

6.2.2.3 POA&Ms

ISSOs are responsible for creating POA&Ms in IACS within 30 days of NFRs being signed by Component management. Because auditors test the effectiveness of controls over the entire fiscal year, it is imperative for remediation of weaknesses identified in IT NFRs to begin as soon as possible. To successfully demonstrate a control has been operating effectively, it must be in place and operating for a sufficient amount of time during the fiscal year being audited. Sufficiency is ultimately determined by the auditor, but they will consider evaluating controls that have been operating for at least 6 months.

7.0 ISSO RECURRING TASKS

This section provides a checklist of tasks an ISSO should perform periodically. Periodicity listed for each task provides general guidelines which may vary depending on Component guidance or individual circumstances. Hard requirements for each task are specified.

7.1 Ongoing Activities

The following activities are required to be completed on a periodic basis (e.g., annually) but need to be worked on throughout the year to ensure they are completed on time:

- Control Assessment
- Review and update the Security Authorization Process documents (i.e., SP, RA, CP and CP Test should be updated as changes occur but each requires an annual update)

7.2 ISSO Weekly activities

- Incident response report (required)
- Check scorecard detail reports
- Review audit logs
- CCB
- Ensure data is backed up
- Check POA&M status. Check daily detail reports in Crystal Reports or see Weakness Search Report Guide attached to the DHS POA&M Guide

7.3 ISSO Monthly activities

- Review scorecard during the third week of the month.
- Review/deactivate unused accounts.

7.4 ISSO Quarterly activities

- Ensure all data in IACS is current and accurate one week before the end of the quarter; DHS submits a quarterly FISMA report to OMB based on this data
- Conduct vulnerability scans

7.5 ISSO annual activities

The following activities need to be completed annually but require an effort over several months to complete:

- Ensure all system users and people with security responsibilities receive their annual awareness training
- Conduct a CP Test

- Ensure vulnerability assessments are completed at least annually
- Conduct vulnerability scans should be conducted at least annually, or when significant changes are made to the system
- Review and validate user access rights

7.6 As Required Activities

- Update SP whenever there are system or personnel changes, but at least annually
- Review the approving change requests
- Participate in the CR process (i.e., reviewing/approving change requests and conducting impact analyses)
- Participate in the development phases of the system life cycle
- Ensure all system users sign the ROB before being granted access

APPENDIX A: REFERENCES

Below is a list of references that provide mandates or guidance that ISSOs need to be aware of:

- Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
- NIST Special Publication (SP) 800-18, Guide for Developing Security Plans for Federal Information Systems
- NIST Special Publication (SP)800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems; A Security Life Cycle Approach
- NIST Special Publication (SP) 800-39, Managing Risk from Information Systems: An Organizational Perspective
- NIST Special Publication (SP) 800-47, Security Guide for Interconnecting Information Technology Systems
- NIST Special Publication (SP) 800-50, Building an Information Technology Security Awareness and Training Program
- NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems
- NIST Special Publication (SP) 800-53A, Guide for Assessing the Security Controls in Federal Information Systems
- NIST Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST Special Publication (SP) 800-63, Electronic Authentication Guideline
- NIST Special Publication (SP) 800-64, Security Considerations in the Information System Development Life Cycle
- NIST Special Publication (SP) 800-100, Information Security Handbook: A Guide for Managers
- DHS 4300A, Sensitive Systems Policy Directive
- DHS 4300A, Sensitive Systems Handbook
    - Attachment B, Waivers and Exceptions Request Form
    - Attachment C, Information Systems Security Officer (ISSO) Designation Letter
    - Attachment D, Type Accreditation
    - Attachment F, Incident Response and Reporting

    - Attachment G, Rules of Behavior
    - Attachment H, Plan of Action and Milestones (POA&M) Process Guide
    - Attachment K, IT Contingency Plan Template
    - Attachment N, Interconnection Security Agreements
    - Attachment R, Compliance Framework for CFO Designated Financial Systems
    - Attachment S, Compliance Framework NIST SP 800-53 Controls for Privacy Sensitive Systems
- DHS Information Security Categorization Guide, FIPS 199 Workbook, and E-Authentication Workbook
- DHS Information Security Categorization Guide, FIPS 199 Workbook, and E-Authentication Workbook
- DHS FISMA System Inventory Methodology
- DHS CISO Directions for the Application of NIST SP 800-53 Rev. 3 Security Controls (tri-fold)
- DHS Document Review Methodology
- FY10 Critical Control Review Methodology
- DHS Critical Control Review Checklist and Sample Slides
- DHS Information Security Strategic Plan 2010 -2014
- Department of Homeland Security
- Information Technology Acquisition Review (ITAR) Quick Essentials Guide
- DHS CIO IT Acquisition Review (ITAR) Guidance
- DHS 4300B, National Security System Policy
- DHS 4300B, National Security Systems Handbook
- DHS 4300C, Sensitive Compartmented Information (SCI) Systems Policy Directive
- DHS SCI Systems Information Assurance Handbook
- DHS Security Architecture
- DHS Security Operations Concept of Operations
- DHS Baseline Configuration documents
- DHS Cisco Router Baseline Configuration
- DHS HP-UX Baseline

- DHS Solaris Baseline Configuration
- DHS Solaris 10 Baseline Configuration
- DHS Linux / SELinux Configuration Guide
- DHS Windows Vista Configuration Guidance
- Appendix A: Vista Computer Configuration Security Settings
- Appendix B: Vista Computer Configuration Other Settings
- DHS Windows XP Baseline Configuration
- DHS Windows Server 2003 Configuration Guidance
- DHS Windows Server 2008 Configuration Guidance
- NSA Guidance -Guide to Securing Microsoft Windows NT Network
- Addendum - NSA Guide to Securing Microsoft Windows NT Networks & NSA Guides to Securing Windows 2000
- Guidance for Securing Windows NT and Server 2000
- Level One Benchmark Windows NT 4-0 Operating Systems

APPENDIX B: ACRONYMS

This Appendix contains a list of Acronyms used in this document

AO	Authorizing Official (formerly DAA)
ATO	Authorization to Operate
CA	Certification Authority
CCB	Configuration Control Board
CERT	Computer Emergency Response Team
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
COE	Common Operating Environment
CP	Contingency Plan
CPIC	Capital Planning and Investment Control
CPT	Contingency Plan Test
CR	Change Request
CSIRC	Computer Security Incident Response Center
CSO	Chief Security Officer
DAA	Designated Accreditating Authority (term is obsolete, replaced byAO)
DBA	Data Base Administrator
DHS	Department Of Homeland Security
DHS SOC	DHS Security Operations Center
DR	Document Review
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FSO	Facility Security Officer
GAO	Government Accountability Office
GSS	General Support System
HSAR	Homeland Security Acquisition Regulation

HSDN	Homeland Secure Data Network
IACS	Information Assurance and Compliance System
IATO	Interim Authorization to Operate
IDS	Intrusion Detection System
ISA	Interconnection Security Agreement
ISSM	Information System Security Manager
ISSO	Information System Security Officer
ISVM	Information Security Vulnerability Management
IT	Information Technology
ITAR	Information Technology Acquisition Review
ITGC	Information Technology General Control
MA	Major Application
MD	Management Directives
MIN	Minor Application
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NFR	Notice of Findings and Recommendations
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
OA	Ongoing Authorization
O&M	Operations and Maintenance
OCISO	Office of the Chief Information Security Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessments
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPOC	Privacy Point of Contact
PTA	Privacy Threshold Analysis
RA	Risk Assessment

RBAC	Role Based Access Control
ROB	Rules of Behavior
ROE	Rules of Engagement
RTM	Requirements Traceability Matrix
SAP	Security Authorization Package
SAR	Security Assessment Report
SBU	Sensitive But Unclassified
SCA	Security Control Assessor
SDLC	System Development Life Cycle
SELC	System Engineering Life Cycle
SLA	Service Level Agreement
SME	Subject Matter Expert
SO	System Owner
SOC	Security Operations Center
SORN	System of Records Notice
SOP	Standard Operating Procedure
SOW	Statement of Work
SP	Special Publication
SP	Security Plan
SUB	Subsystem
TOD	Test of Design
TOE	Test of Effectiveness
TYP	Type Accredited System
UPS	Uninterruptible Power Supply

APPENDIX C: OIG POTENTIAL LISTING OF SECURITY TEST TOOLS & UTILITIES

The following is a list of the potential OIG tools/utilities available for use during testing. Any additional tools must be approved by the OIG and Component TPOC prior to use.

Primary Tools	
NMAP	Firefox
VMware Player or Workstation with Backtrack 4	Oracle Auditing Tools
AppDetectivePro	Java
Nessus 4	Putty
Metasploit	snmpwalk
Microsoft Baseline Security Analyzer	Ifran View
Secondary Tools	
iSQLw (Microsoft's SQL client available on the MS-SQL install CD)	PSTools
Scuba	Oracle Assessment Kit
ParosProxy	Spork
ActivePerl	Fgdump or PWdumpX
Wikto/Skilly/Spud (all from www.sensepost.com)	John the Ripper with Multipatch
Cain and Abel	FileZilla
Wireshark	ldp.exe Windows Server 2003 Support Tools
VIM	Nipper
Athena's Firewall Browser	IBM DB2 Client Drivers
Oracle Thin JDBC Drive	