



**Homeland
Security**

DHS 4300A Sensitive Systems Handbook

Attachment M

Tailoring NIST 800-53 Security Controls

Version 11.0
August 5, 2014

Protecting the Information that Secures the Homeland

This page intentionally blank

Document Change History

Version	Date	Description
4.0	June 1, 2006	Initial Release
5.0	March 1, 2007	No Change
5.5	September 30, 2007	Updated Excel spreadsheet named M – 800-53 Controls to include control enhancements. Updated date and version number to coincide with current Handbook.
6.0	May 14, 2008	No Change
6.1	September 23, 2008	No Change
7.0	August 7, 2009	No Change
7.1	June 21, 2010	Major update to Excel object to bring in line with NIST SP 800-53, Rev 3. Combined both worksheets.
9.1	July 24, 2012	
11.0	February 28, 2014	Rewritten as new document. Substantial revision to the Excel spreadsheet object according to NIST SP 800-53 Revision 4. Introductory text and tailoring process explanation also updated to reflect the expanded tailoring guidance provided in Rev 4.

CONTENTS

1.0	Introduction	1
2.0	Tailoring the NIST SP 800-53 Controls.....	1
2.1	<i>The Tailoring Process.....</i>	<i>1</i>
2.1.1	Identifying and Designating Common Controls	1
2.1.2	Applying Scoping Considerations.....	2
2.1.3	Selecting Compensating Security Controls	3
2.1.4	Assigning Security Control Parameter Values.....	3
2.1.5	Supplementing Security Control Baselines	3
2.1.6	Providing Additional Specification Information.....	4
2.2	<i>Control-Specific Tailoring Guidance.....</i>	<i>4</i>

1.0 INTRODUCTION

National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publications (FIPS PUB) are standards adopted and promulgated under the provisions of Section 5131 of the Information Technology Management Reform Act of 1996, Public Law (P.L.) 104-106, and the Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347.

In particular, FIPS PUB 199, “Standards for Security Categorization of Federal Information and Information Systems,” directs Federal Government organizations to categorize their information systems as low, moderate, or high impact for each of the three information security objectives (confidentiality, integrity, and availability). The overall impact categorization of a system is generally equal to the highest impact assigned to any of the three objectives (high-water mark); however, this is not necessarily the case for DHS systems.

DHS amplifies the FIPS PUB 199 high-water mark requirement to reflect actual security requirements, a Department-level risk-based decision that is consistent with FISMA policy, which requires Federal agencies to “cost-effectively reduce information security risks to an acceptable level.”¹ The policy amplification is also consistent with the NIST information security guidance that promotes the concept of “risk-based decisions.”

Controls tailoring, and use of compensating controls, is also consistent with providing the safeguards necessary to reduce the risks in a specific operational environment. A system thus has the controls necessary to meet its security objectives without implementing unnecessary controls; however, any program may implement additional controls when deemed appropriate.

When selecting security controls using risk-based decisions, it is important to have all pertinent information and to have clearly defined and documented risks for a particular system. This will enable Authorizing Officials (AO) to make informed decisions on the acceptable risk level for a specific system in an explicit operational environment.

¹ FISMA §3544.(b)(2)(B)

2.0 TAILORING THE NIST SP 800-53 CONTROLS

NIST SP 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” Revision 4, April 2013, provides expanded, updated, and streamlined security control tailoring guidance and the potential use of specialized control overlays, based upon a risk assessment. The FIPS PUB 199 characterization of a system for confidentiality, integrity, and availability, and tailoring of the NIST SP 800-53 controls, will ensure that implemented controls provide sufficient safeguards.

2.1 The Tailoring Process

“The tailoring process includes:

- Identifying and designating common controls in initial security control baselines;
- Applying scoping considerations to the remaining baseline security controls;
- Selecting compensating security controls, if needed;
- Assigning specific values to organization-defined security control parameters via explicit assignment and selection statements;
- Supplementing baselines with additional security controls and control enhancements, if needed; and
- Providing additional specification information for control implementation, if needed.”²

Important note: As per NIST SP 800-53 guidance for tailoring the baseline controls:

“... organizations do not remove security controls for operational convenience. Tailoring decisions regarding security controls should be defensible based on mission/business needs and accompanied by explicit risk-based determinations.”³

The following sections summarize the tailoring considerations located in Section 3 of NIST SP 800-53, Rev 4.

2.1.1 Identifying and Designating Common Controls

Some systems may inherit all or some controls from other systems or facilities, i.e. from a General Support System or from a data center or server farm. Each condition must be evaluated on a case by case basis to determine whether inherited

² NIST SP 800-53 Section 3.2, page 30.

³ NIST SP 800-53 Section 3.2, page 31, paragraph 2.

controls adequately address system requirements. This can potentially reduce the overall resource expenditures by organizations.

2.1.2 Applying Scoping Considerations

Components may scope individual system requirements by selecting and applying only those controls from the initial security control baselines that provide adequate safeguards based on the system mission, business function, the environment in which it operates, and the Component's risk tolerance. Scoping considerations shall be accounted for in the security plan.

Considerations include:

- Control Allocation and Placement
- Implementation of Compensating Security Controls
- Operational and Environmental Concerns

Some factors include:

- Mobility
 - Single-User Systems and Operations
 - Data Connectivity and Bandwidth
 - Limited Functionality Systems or System Components
 - Information and System Non-Persistence
 - Public Access
- Security Objective

Security controls that support only one or two of the confidentiality, integrity, or availability security objectives may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if not defined in a lower baseline) only if the downgrading action:

1. Reflects the FIPS PUB 199 security category for the supported security objective(s) before moving to the FIPS PUB 200 impact level (i.e., high-water mark);
 2. Is supported by an organizational assessment of risk; and
 3. Does not adversely affect the level of protection for the security-relevant information within the information system.
- Technology

Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) are applicable only if those technologies are employed or are required to be employed within organizational information systems. Security controls that can be explicitly or implicitly supported by automated mechanisms do not require the development of such mechanisms if the mechanisms do not already exist or are not readily available in commercial or government off-the-shelf products. If automated mechanisms are not readily available, cost-effective, or technically feasible, compensating security controls, implemented through non-automated mechanisms or procedures, are used to satisfy specified security controls or control enhancements (see terms and conditions for applying compensating controls below).

- **Mission Requirements**

Some security controls may be inappropriate if they degrade, debilitate, or otherwise hamper critical organizational missions and/or business functions.

2.1.3 Selecting Compensating Security Controls

Components may employ alternative security controls that provide equivalent or comparable protection when, due to the specific nature of the information systems or environment results in a baseline control that is not a cost-effective means of obtaining the needed risk mitigation. The use of compensating controls shall be accounted for in the Security Plan.

Components may employ compensating controls:

- From NIST SP 800-53 Appendix F; if appropriate compensating controls are unavailable, organizations may adopt suitable compensating controls from other sources;
- With supporting rationale for how the compensating control provides equivalent security and why the baseline security control could not be employed; and
- By accepting the risk for their deployment.

2.1.4 Assigning Security Control Parameter Values

Components must review the security controls (and enhancements) for assignment/selection statements and define values for each parameter. These parameter values become a part of the security control requirement for that system. Note: Parameter values may be prescribed by applicable federal laws, Executive Orders, directives, regulations, policies or standards.

2.1.5 Supplementing Security Control Baselines

In some cases, additional safeguards beyond those contained in the baselines will be required to address specific threats to and vulnerabilities in organizations,

mission/business processes, and/or information systems and to satisfy the requirements of applicable federal laws, Executive Orders, directives, policies, standards, or regulations.

Some situations which may require baseline supplementation:

- Advanced persistent threat;
- Cross-domain services;
- Mobility;
- Personally Identifiable Information (PII);
- Financial Data; and
- Classified information.

2.1.6 Providing Additional Specification Information for Control Implementation

Additional detail may be necessary to fully define the intent of a security control, e.g., directions on how to apply the control in different situations. Components may determine whether or not to include additional implementation data, but may not change the intent of the security control or modify the original language in the control.

2.2 Control-Specific Tailoring Guidance

A security control baseline spreadsheet is appended to this document. The spreadsheet identifies the impact level (L = low, M = moderate, and H = high) and security objective(s) (C = confidentiality, I = integrity, and A = availability) for each NIST SP 800-53 control and provides guidance on the possible tailoring of these controls.



NIST SP 800-53
Tailoring.xlsx