DRAFT – this is neither a NIST-owned nor a NIST-approved document: Restricted circulation

NIST Special Publication 800-53
Revision 2 - ***Proposed text***
(***final version v1 - 2008-04-03***)

Recommended Security Controls for Federal Information Systems

(with Annex J)

Ron Ross
Stu Katzke
Arnold Johnson
Marianne Swanson
Gary Stoneburner
George Rogers
Richard Wilsher

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

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

~~December 2006~~ mnth 2008

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

Technology Administration
Robert Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director

Reports on Computer Systems Technology

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

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by ~~federal~~Federal agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on ~~federal~~Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other ~~federal~~Federal official.

NIST Special Publication 800-53, Revision ~~1~~2, ~~167~~ 225 pages

(~~December 2006~~ mnth 2008) CODEN: NSPUE2

There are references in this publication to documents currently under development by NIST in accordance with responsibilities assigned to NIST under the Federal Information Security Management Act of 2002. The methodologies in this document may be used even before the completion of such companion documents. Thus, until such time as each document is completed, current requirements, guidelines, and procedures (where they exist) remain operative. For planning and transition purposes, agencies may wish to closely follow the development of these new documents by NIST. Individuals are also encouraged to review the public draft documents and offer their comments to NIST. All NIST documents mentioned in this publication, other than the ones noted above, are available at http://csrc.nist.gov/publications.

COMMENTS MAY BE SUBMITTED TO THE COMPUTER SECURITY DIVISION, INFORMATION TECHNOLOGY LABORATORY, NIST VIA ELECTRONIC MAIL AT SEC-CERT@NIST.GOV OR VIA REGULAR MAIL AT
100 BUREAU DRIVE (MAIL STOP 8930) GAITHERSBURG, MD 20899-8930

Table of Contents

CHAPTER ONE

INTRODUCTION

THE NEED FOR SECURITY CONTROLS TO PROTECT INFORMATION SYSTEMS

The selection and employment of appropriate *security controls* for an information system[1] are important tasks that can have major implications on the operations[2] and assets of an organization as well as the welfare of individuals. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. There are several important questions that should be answered by organizational officials when addressing the security considerations for their information systems:

- What security controls are needed to adequately protect the information systems that support the operations and assets of the organization in order for that organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals?
- Have the selected security controls been implemented or is there a realistic plan for their implementation?
- What is the desired or required level of assurance (i.e., grounds for confidence) that the selected security controls, as implemented, are effective[3] in their application?

The answers to these questions are not given in isolation but rather in the context of an effective *information security program* for the organization that identifies, controls, and mitigates risks to its information and information systems.[4] The security controls defined in Special Publication 800-53 and recommended for use by organizations in protecting their information systems should be employed in conjunction with and as part of a well-defined and documented information security program. An effective information security program should include:

- Periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization;
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level and address information security throughout the life cycle of each organizational information system;

[1] An information system is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial/process controls systems, telephone switching/private branch exchange (PBX) systems, and environmental control systems.

[2] Organizational operations include mission, functions, image, and reputation.

[3] Security control effectiveness addresses the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment.

[4] The E-Government Act (P.L. 107-347), passed by the one hundred and seventh Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.

- Plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization;
- Procedures for detecting, reporting, and responding to security incidents; and
- Plans and procedures for continuity of operations for information systems that support the operations and assets of the organization.

It is of paramount importance that responsible officials within the organization understand the risks and other factors that could adversely affect organizational operations, organizational assets, or individuals. Moreover, these officials must understand the current status of their security programs and the security controls planned or in place to protect their information systems in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the organization and to accomplish the organization’s stated mission(s) with what the Office of Management and Budget (OMB) Circular A-130 defines as *adequate security*, or security commensurate with risk, including the magnitude of harm to individuals, the organization, or its assets resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the ~~federal~~Federal government. The guidelines apply to all components[5] of an information system that process, store, or transmit ~~federal~~Federal information. The guidelines have been developed to help achieve more secure information systems within the ~~federal~~Federal government by:

- Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems;
- Providing a recommendation for minimum security controls for information systems categorized in accordance with Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*;

[5] Information system components include, but are not limited to, mainframes, servers, workstations, network components, operating systems, middleware, and applications. Network components can include, for example, such devices as firewalls, sensors (local or remote), switches, guards, routers, gateways, wireless access points, and network appliances. Servers can include, for example, database servers, authentication servers, electronic mail and web servers, proxy servers, domain name servers, and network time servers. Information system components are either purchased commercially off-the-shelf or are custom-developed and can be deployed in land-based, sea-based, airborne, and/or space-based information systems.

- Providing a stable, yet flexible catalog of security controls for information systems to meet current organizational protection needs and the demands of future protection needs based on changing requirements and technologies; and
- Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness.

The guidelines provided in this special publication are applicable to all ~~federal~~Federal information systems[6] other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542.[7] The guidelines have been broadly developed from a technical perspective to complement similar guidelines for national security systems. This publication is intended to provide guidance to ~~federal~~Federal agencies implementing FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. In addition to the agencies of the ~~federal~~Federal government, state, local, and tribal governments, and private sector organizations that compose the critical infrastructure of the United States, are encouraged to use these guidelines, as appropriate.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse ~~federal~~Federal audience of information system and information security professionals including: (i) individuals with information system and information security management and oversight responsibilities (e.g., chief information officers, senior agency information security officers, and authorizing officials); (ii) individuals with information system development responsibilities (e.g., program and project managers, mission/application owners, system designers, system and application programmers); (iii) individuals with information security implementation and operational responsibilities (e.g., information system owners, information owners, information system administrators, information system security officers,); and (iv) individuals with information system and information security assessment and monitoring responsibilities (e.g., auditors, inspectors general, evaluators, and certification agents). Commercial companies producing information technology products and systems, creating information security-related technologies, and providing information security services can also benefit from the information in this publication.

1.3 RELATIONSHIP TO OTHER SECURITY CONTROL PUBLICATIONS

To create the most technically sound and broadly applicable set of security controls for information systems, a variety of sources were considered during the development of this special publication. The sources included security controls from the defense, audit, financial, healthcare, and intelligence communities as well as controls defined by national and international standards organizations.[8] The objective of NIST Special Publication 800-53 is to provide a set of security

[6] A ~~federal~~Federal information system is an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

[7] NIST Special Publication 800-59 provides guidance on identifying an information system as a national security system.

[8] Security controls from the audit, defense, healthcare, intelligence, and standards communities are contained in the following publications: (i) Government Accountability Office, *Federal Information System Controls Audit Manual*; (ii) Department of Defense Instruction 8500.2, *Information Assurance Implementation*; (iii) Department of Health and Human Services Centers for Medicare and Medicaid Services, *Core Security Requirements*; (iv) Director of Central Intelligence Directive 6/3 Manual, *Protecting Sensitive Compartmented Information within Information Systems*; (v) NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*; and (vi) International Organization for Standardization/International Electrotechnical Commission 17799:2005, *Code of Practice for Information Security Management*.

controls that is sufficiently rich to satisfy the breadth and depth of security requirements[9] levied on information systems and that is consistent with and complementary to other established security standards.

The catalog of security controls provided in Special Publication 800-53 can be effectively used to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements. It is the responsibility of organizations to select the appropriate security controls, to implement the controls correctly, and to demonstrate the effectiveness of the controls in satisfying their stated security requirements. The security controls in the catalog facilitate the development of assessment methods and procedures that can be used to demonstrate control effectiveness in a consistent and repeatable manner—thus contributing to the organization's confidence that there is ongoing compliance with its stated security requirements.[10]

1.4 ORGANIZATIONAL RESPONSIBILITIES

Organizations[11] should use FIPS 199 to define security categories for their information systems. This publication associates recommended minimum security controls with FIPS 199 low-impact, moderate-impact, and high-impact security categories. For each information system, the recommendation for minimum security controls from Special Publication 800-53 (i.e., the baseline security controls defined in Appendix D, tailored in accordance with the tailoring guidance in Section 3.3) is intended to be used as a starting point for and input to the organization's risk assessment process.[12] The risk assessment results are used to supplement the tailored baseline resulting in a set of agreed-upon controls documented in the security plan for the information system. While the FIPS 199 security categorization associates the operation of the information system with the potential impact on an organization's operations, assets, or individuals, the incorporation of refined threat and vulnerability information during the risk assessment facilitates supplementing the tailored baseline security controls to address organizational needs and tolerance for risk. The final, agreed-upon set of security controls should be documented with appropriate rationale in the security plan for the information system.[13]

The use of security controls from Special Publication 800-53 and the incorporation of tailored baseline controls as a starting point in the control selection process, facilitates a more consistent level of security across ~~federal~~Federal information systems. It also offers the needed flexibility to

[9] Security requirements are those requirements levied on an information system that are derived from laws, Executive Orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

[10] NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft), April 2006, provides guidance on assessment methods and procedures for security controls defined in this publication. Special Publication 800-53A can also be used to conduct self-assessments of information systems.

[11] An organization typically exercises direct managerial, operational, and/or financial control over its information systems and the security provided to those systems, including the authority and capability to implement the appropriate security controls necessary to protect organizational operations, organizational assets, and individuals.

[12] Risk assessments can be accomplished in a variety of ways depending on the specific needs of the organization. The assessment of risk is a process that should be incorporated into the system development life cycle. NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, provides guidance on the assessment and mitigation of risk as part of an overall risk management process.

[13] NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, provides guidance on documenting information system security controls. The general guidance in Special Publication 800-18 is augmented by Special Publication 800-53 with recommendations for information and rationale to be included in the system security plan.

appropriately modify the controls based on specific organizational policy and requirements, particular conditions and circumstances, known threat and vulnerability information, and tolerance for risk to the organization's operations, assets, or to individuals.

Building a more secure information system is a multifaceted undertaking that involves the use of: (i) well-defined system-level security requirements and security specifications; (ii) well-designed information technology products; (iii) sound systems/security engineering principles and practices to effectively integrate information technology products into the information system; (iv) appropriate methods for product/system testing and evaluation; and (v) comprehensive system security planning and life cycle management.[14] From a systems engineering viewpoint, security is just one of many required capabilities for an organizational information system—capabilities that must be funded by the organization throughout the life cycle of the system. Realistically assessing the risks to an organization's operations and assets or to individuals by placing the information system into operation or continuing its operation is of utmost importance. Addressing the information system security requirements must be accomplished with full consideration of the risk tolerance of the organization in light of the potential impacts, cost, schedule, and performance issues associated with the acquisition, deployment, and operation of the system.

1.5 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the fundamental concepts associated with security control selection and specification including: (i) the structural components of security controls and how the controls are organized into families; (ii) minimum (baseline) security controls; (iii) the use of common security controls in support of organization-wide information security programs; (iv) security controls in external environments; (v) assurance in the effectiveness of security controls; and (vi) the commitment to maintain currency of the individual security controls and the control baselines.

- **Chapter Three** describes the process of selecting and specifying security controls for an information system including: (i) defining the organization's overall approach to managing risk; (ii) categorizing the system in accordance with FIPS 199; (iii) selecting and tailoring the initial set of minimum (baseline) security controls; (iv) supplementing the tailored security control baseline, as necessary, based upon risk assessment results; and (v) updating the controls as part of a comprehensive continuous monitoring process.

- **Supporting appendices** provide more detailed security control selection and specification-related information including: (i) general references; (ii) definitions and terms; (iii) acronyms; (iv) baseline security controls for low-impact, moderate-impact, and high-impact information systems; (v) minimum assurance requirements; (vi) a master catalog of security controls; (vii) mapping tables relating the security controls in this publication to other standards and control sets; (viii) crosswalks of NIST security standards and guidelines with associated security controls; and (ix) guidance on the application of security controls to industrial control systems.

[14] Successful life cycle management depends on having qualified personnel to oversee and manage the information systems within an organization. The skills and knowledge of organizational personnel with information systems (and information security) responsibilities should be carefully evaluated (e.g., through performance, certification, etc.).

CHAPTER TWO

THE FUNDAMENTALS

SECURITY CONTROL STRUCTURE, ORGANIZATION, BASELINES, AND ASSURANCE

This chapter presents the fundamental concepts associated with security control selection and specification including: (i) the structure of security controls and the organization of the controls in the control catalog; (ii) security control baselines; (iii) the identification and use of common security controls; (iv) security controls in external environments; (v) security control assurance; and (vi) future revisions to the security controls, the control catalog, and baseline controls.

2.1 SECURITY CONTROL ORGANIZATION AND STRUCTURE

Security controls in the security control catalog (Appendix F) have a well-defined organization and structure. The security controls are organized into *classes* and *families* for ease of use in the control selection and specification process. There are three general classes of security controls (i.e., management, operational, and technical) and seventeen security control families.[15] Each family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each control family. Table 1 summarizes the classes and families in the security control catalog and the associated family identifiers.

TABLE 1: SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS

IDENTIFIER	FAMILY	CLASS		
AC	Access Control			Technical
AT	Awareness and Training		Operational	
AU	Audit and Accountability			Technical
CA	Certification, Accreditation, and Security Assessments	Management		
CM	Configuration Management		Operational	
CP	Contingency Planning		Operational	
IA	Identification and Authentication			Technical
IR	Incident Response		Operational	
MA	Maintenance		Operational	
MP	Media Protection		Operational	
PE	Physical and Environmental Protection		Operational	
PL	Planning	Management		
PS	Personnel Security		Operational	
RA	Risk Assessment	Management		
SA	System and Services Acquisition	Management		
SC	System and Communications Protection			Technical
SI	System and Information Integrity		Operational	

To uniquely identify each control, a numeric identifier is appended to the family identifier to

[15] The seventeen security control families in NIST Special Publication 800-53 are closely aligned with the seventeen security-related areas in FIPS 200 specifying the minimum security requirements for protecting ~~federal~~Federal information and information systems. Families are assigned to their respective classes based on the dominant characteristics of the controls in that family. Many security controls, however, can be logically associated with more than one class. For example, CP-1, the policy and procedures control from the Contingency Planning family, is listed as an operational control but also has characteristics that are consistent with security management as well.

indicate the number of the control within the control family. For example, CP-9 is the ninth control in the Contingency Planning family.

The security control structure consists of three key components: (i) a *control* section; (ii) a *supplemental guidance* section; and (iii) a *control enhancements* section.[16] The following example from the Auditing and Accountability family illustrates the structure of a typical security control.

AU-2 AUDITABLE EVENTS

Control: The information system generates audit records for the following events: [*Assignment: organization-defined auditable events*].

Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST Special Publication 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The information system provides the capability to compile audit records from multiple components throughout the system into a systemwide (logical or physical), time-correlated audit trail.

(2) The information system provides the capability to manage the selection of events to be audited by individual components of the system.

(3) The organization periodically reviews and updates the list of organization-defined auditable events.

LOW AU-2	**MOD** AU-2 (3)	**HIGH** AU-2 (1) (2) (3)

The control section provides a concise statement of the specific security capability needed to protect a particular aspect of an information system. The control statement describes specific security-related activities or actions to be carried out by the organization or by the information system. For some controls in the control catalog, a degree of flexibility is provided by allowing organizations to selectively define input values for certain parameters associated with the controls. This flexibility is achieved through the use of *assignment* and *selection* operations within the main body of the control. Assignment and selection operations provide an opportunity for an organization to tailor the security controls to support specific mission, business, or operational needs. For example, an organization can specify the specific events to be audited. Once specified, the organization-defined value becomes part of the control, and the organization is assessed against the completed control statement. Some assignment operations may specify minimum or maximum values that constrain the values that may be input by the organization.

[16] A supplemental guidance section is also used for security control enhancements in situations where the guidance is not generally applicable to the entire control but instead focused on the particular control enhancement.

Selection statements also narrow the potential input values by providing a specific list of items from which the organization must choose.

The supplemental guidance section provides additional information related to a specific security control. Organizations are expected to apply the supplemental guidance as appropriate, when defining, developing, and implementing security controls. In certain instances, the supplemental guidance provides more detail concerning the control requirements or important considerations (and the needed flexibility) for implementing security controls in the context of an organization's operational environment, specific mission requirements, or assessment of risk. In addition, applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance documents (e.g., OMB Circulars, FIPS, and NIST Special Publications) are listed in the supplemental guidance section, when appropriate, for the particular security control.

The control enhancements section provides statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control. In both cases, the control enhancements are used in an information system requiring greater protection due to the potential impact of loss or when organizations seek additions to a basic control's functionality based on the results of a risk assessment. Control enhancements are numbered sequentially within each control so that the enhancements can be easily identified when selected to supplement the basic control. In the example above, if all three control enhancements are selected, the control designation subsequently becomes AU-2 (1) (2) (3). The numerical designation of a security control enhancement is used only to identify a particular enhancement within the control structure. The designation is neither indicative of the relative strength of the control enhancement nor assumes any hierarchical relationship among enhancements. In the above example, enhancement (3) is used before (1) and (2) since that enhancement is appropriate at a lower level than the other two. This type of situation arises from the decision to enhance control stability in the face of change by not renumbering existing enhancements when new ones are added or when decisions about placement within baselines change.

2.2 SECURITY CONTROL BASELINES

Organizations are required to employ security controls to meet security requirements defined by applicable laws, Executive Orders, directives, policies, standards, or regulations (e.g., Federal Information Security Management Act, OMB Circular A-130, Appendix III). The challenge for organizations is to determine the appropriate set of security controls, which if implemented and determined to be effective in their application, would most cost-effectively comply with the stated security requirements.[17] Selecting the appropriate set of security controls to meet the specific, and sometimes unique, security requirements of an organization is an important task—a task that demonstrates the organization's commitment to security and the due diligence exercised in protecting the confidentiality, integrity, and availability of their information and information systems.

To assist organizations in making the appropriate selection of security controls for their information systems, the concept of *baseline* controls is introduced. Baseline controls are the minimum security controls recommended for an information system based on the system's

[17] An information system may require security controls at different layers within the system. For example, an operating system or network component typically provides an identification and authentication capability. An application may also provide its own identification and authentication capability rendering an additional level of protection for the overall information system. The selection and specification of security controls should consider components at all layers within the information system as part of effective security and privacy architectures.

security categorization in accordance with FIPS 199.[18] The tailored security control baseline (i.e., the appropriate control baseline from Appendix D tailored in accordance with the guidance in Section 3.3) serves as the *starting point* for organizations in determining the appropriate safeguards and countermeasures necessary to protect their information systems. Because the baselines are intended to be broadly applicable starting points, supplements to the tailored baselines (see Section 3.4) will likely be necessary in order to achieve adequate risk mitigation. The tailored baselines are supplemented based on organizational assessments of risk and the resulting controls documented in the security plans for the information systems.

Appendix D provides a listing of baseline security controls. Three sets of baseline controls have been identified corresponding to the low-impact, moderate-impact, and high-impact levels defined in the security categorization process in FIPS 199 and derived in Section 3.2. Each of the three baselines provides an initial set of security controls for a particular impact level associated with a security category.[19] Appendix F provides the complete catalog of security controls for information systems, arranged by control families. The catalog represents the entire set of security controls defined at this time. Chapter 3 provides additional information on how to use security categories to select the appropriate set of baseline security controls, how to apply the tailoring guidance to the baseline controls, and how to supplement the tailored baseline in order to achieve adequate risk mitigation.

Implementation Tip

Since the baseline security controls represent the minimum controls for low-impact, moderate-impact, and high-impact information systems, respectively, there are additional controls and control enhancements that appear in the catalog that are found in only higher-impact baselines or not used in any of the baselines. These additional security controls and control enhancements for the information system are available to organizations and can be used in supplementing the tailored baselines to achieve the needed level of protection in accordance with an organizational assessment of risk. Moreover, security controls and control enhancements contained in higher-level baselines can also be used by organizations to strengthen the level of protection provided in lower-level baselines, if deemed appropriate. At the end of the security control selection and specification process, the agreed-upon set of security controls documented in the security plan, must be sufficient to provide adequate security for the organization and mitigate risks to its operations, assets, and individuals.

2.3 COMMON SECURITY CONTROLS

An organization-wide view of an information security program facilitates the identification of *common security controls* that can be applied to one or more organizational information systems. Common security controls can apply to: (i) all organizational information systems; (ii) a group of information systems at a specific site; or (iii) common information systems, subsystems, or applications (i.e., common hardware, software, and/or firmware) deployed at multiple operational sites. Common security controls have the following properties:

- The development, implementation, and assessment of common security controls can be assigned to responsible organizational officials or organizational elements (other than the

[18] FIPS 199 security categories are based on the potential impact on an organization or individuals should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

[19] The baseline security controls contained in Appendix D are not necessarily absolutes in that the tailoring guidance described in Section 3.3 provides the organization the ability to eliminate certain controls or specify compensating controls under strict terms and conditions.

information system owners whose systems will implement or use the common security controls); and

- The results from the assessment of the common security controls can be used to support the security certification and accreditation processes of organizational information systems where the controls have been applied.[20]

The identification of common security controls is most effectively accomplished as an organization-wide exercise with the involvement of the chief information officer, senior agency information security officer, authorizing officials, information system owners/program managers, information owners, and information system security officers. The organization-wide exercise considers the categories of information systems within the organization in accordance with FIPS 199 (i.e., low-impact, moderate-impact, or high-impact information systems) and the minimum security controls necessary to protect the operations and assets supported by those systems (see *baseline* security controls in Section 2.2). For example, common security controls can be identified for all low-impact information systems by considering the baseline security controls for that category of information system. Similar exercises can be conducted for moderate-impact and high-impact systems as well.

Many of the security controls needed to protect an information system (e.g., contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls) may be excellent candidates for common security control status. By centrally managing the development, implementation, and assessment of the common security controls designated by the organization, security costs can be amortized across multiple information systems. Security controls not designated as common controls are considered *system-specific controls* and are the responsibility of the information system owner. Security plans for individual information systems should clearly identify which security controls have been designated by the organization as common security controls and which controls have been designated as system-specific controls.

Organizations may also assign a *hybrid* status to security controls in situations where one part of the control is deemed to be common, while another part of the control is deemed to be system-specific. For example, an organization may view the IR-1 (Incident Response Policy and Procedures) security control as a hybrid control with the policy portion of the control deemed to be common and the procedures portion of the control deemed to be system-specific. Hybrid security controls may also serve as templates for further control refinement. An organization may choose, for example, to implement the CP-2 (Contingency Planning) security control as a master template for a generalized contingency plan for all organizational information systems with individual information system owners tailoring the plan, where appropriate, for system-specific issues.

Information system owners are responsible for any system-specific issues associated with the implementation of an organization's common security controls. These issues are identified and described in the system security plans for the individual information systems. The senior agency information security officer, acting on behalf of the chief information officer, should coordinate with organizational officials (e.g., facilities managers, site managers, personnel managers) responsible for the development and implementation of the designated common security controls to ensure that the required controls are put into place, the controls are assessed, and the

[20] NIST Special Publication 800-37 provides guidance on security certification and accreditation of information systems.

assessment results are shared with the appropriate information system owners to better support the security accreditation process.

Partitioning security controls into common controls and system-specific controls can result in significant savings to the organization in development and implementation costs especially when the common controls serve multiple information systems and entities. It can also result in a more consistent application of the security controls across the organization at large. Moreover, equally significant savings can be realized in the security certification and accreditation process. Rather than assessing common security controls in every information system, the certification process draws upon any applicable results from the most current assessment of the common security controls performed at the organization level. An organization-wide approach to reuse and sharing of assessment results can greatly enhance the efficiency of the security certifications and accreditations being conducted by organizations and significantly reduce security program costs.

While the concept of security control partitioning into common security controls and system-specific controls is straightforward and intuitive, the application of this principle within an organization takes planning, coordination, and perseverance. If an organization is just beginning to implement this approach or has only partially implemented this approach, it may take some time to get the maximum benefits from security control partitioning and the associated reuse of assessment evidence. Because of the potential dependence on common security controls by many of an organization's information systems, a failure of such common controls may result in a significant increase in agency-level risk—risk that arises from the operation of the systems that depend on these controls.

Implementation Tip

The FIPS 199 security categorization process and the selection of common security controls are closely related activities that are most effectively accomplished on an organization-wide basis with the involvement of the organization's senior leadership (i.e., authorizing officials, chief information officer, senior agency information security officer, information system owners, and mission/information owners). These individuals have the collective corporate knowledge to understand the organization's priorities, the importance of the organization's operations (including mission, functions, image, and reputation) and assets, and the relative importance of the organizational information systems that support those operations and assets. The organization's senior leaders are also in the best position to select the common security controls for each of the security control baselines and assign organizational responsibilities for developing, implementing, and assessing those controls.

2.4 SECURITY CONTROLS IN EXTERNAL ENVIRONMENTS

Organizations are becoming increasingly reliant on information system services provided by external service providers to carry out important missions and functions. External information system services are services that are implemented outside of the system's accreditation boundary (i.e., services that are used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business[21] arrangements), licensing agreements, and/or supply

[21] In March 2004, OMB initiated a governmentwide analysis of selected lines of business supporting the President's Management Agenda goal to expand Electronic Government. Interagency task forces examined business and information technology data and best practices for each line of business—Case Management, Financial Management, Grants Management, Human Resources Management, Federal Health Architecture, Information Systems Security, Budget Formulation and Execution, Geospatial, and IT Infrastructure. The goal of the effort is to identify opportunities to reduce the cost of government and improve services to citizens through business performance improvements.

chain exchanges. The growing dependence on external service providers and new relationships being forged with those providers present new and difficult challenges for the organization, especially in the area of information system security. These challenges include, but are not limited to: (i) defining the types of external services provided to the organization;[22] (ii) describing how the external services are protected in accordance with the security requirements of the organization; and (iii) obtaining the necessary assurances that the risk to the organization's operations and assets, and to individuals, arising from the use of the external services is at an acceptable level.

The assurance or confidence that the risk to the organization's operations, assets, and individuals is at an acceptable level depends on the trust[23] that the authorizing official places in the external service provider. In some cases, the level of trust is based on the amount of direct control the authorizing official is able to exert on the external service provider with regard to the employment of appropriate security controls necessary for the protection of the service and the evidence brought forth as to the effectiveness of those controls. The level of control is usually established by the terms and conditions of the contract or service-level agreement with the external service provider and can range from extensive (e.g., negotiating a contract or agreement that specifies detailed security control requirements for the provider[24]) to very limited (e.g., using a contract or service-level agreement to obtain commodity services[25] such as commercial telecommunications services). In other cases, the level of trust is derived from other factors that convince the authorizing official that the requisite security controls have been employed and that a credible determination of control effectiveness exists. For example, a separately accredited external information system service provided to a ~~federal~~Federal agency through a line of business relationship may provide a degree of trust in the external service within the tolerable risk range of the authorizing official.

[22] Information exchanges may be required among the many possible relationships with external service providers. The risk of exchanging information among business partners and other external entities must be assessed and appropriate security controls employed. There may be contract language that establishes specific requirements to protect information exchanged and/or that specifies particular remedies for failure to protect the information as prescribed. In addition, there may be laws or regulations that protect this information from unauthorized disclosure.

[23] The level of trust that an organization places in an external service provider can vary widely ranging from those who are highly trusted (e.g., business partners in a joint venture that share a common business model and common goals) to those who are less trusted and represent greater sources of risk (e.g., business partners in one endeavor who are also competitors in another market sector).

[24] In reality, the provision of services by providers external to the organization may result in some services without explicit agreements between the organization and the external entities responsible for the services. Whenever explicit agreements are feasible and practical (e.g., through contracts, service-level agreements, etc.), the organization should develop such agreements and require the use of the security controls in Special Publication 800-53. When the organization is not in a position to require explicit agreements with external service providers (e.g., when the service is imposed on the organization or when the service is commodity service), the organization should establish explicit assumptions about the service capabilities with regard to security. Contracts between the organization and external service providers may also require the active participation of the organization. For example, the organization may be required by the contract to install public key encryption-enabled client software recommended by the service provider.

[25] Normally, commercial providers of commodity-type services (e.g., telecommunications services) organize their business models and services around the concept of shared resources and devices for a broad and diverse customer base. Therefore, unless organizations obtain fully dedicated services from commercial service providers (including dedicated devices and management systems), there will likely be a need for greater reliance on compensating security controls to provide the necessary protections for the information system that relies on those external services. The organization's risk assessment and risk mitigation activities should reflect this situation.

Ultimately, the responsibility for adequately mitigating risks to the organization's operations and assets, and to individuals, arising from the use of external information system services remains with the authorizing official. Authorizing officials must require that an appropriate *chain of trust* be established with external service providers when dealing with the many issues associated with information system security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. The chain of trust can be very complicated due to the number of entities participating in the consumer-provider relationship and the type of relationship between the parties. External service providers may also in turn outsource the services to other external entities, making the chain of trust even more complicated and difficult to manage. Depending on the nature of the service, it may simply be unwise for the organization to wholly trust the provider—not due to any inherent untrustworthiness on the provider's part, but due to the intrinsic level of risk in the service. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating controls or accepts the greater degree of risk to its operations and assets, or to individuals.

2.5 SECURITY CONTROL ASSURANCE

Assurance is the grounds for confidence[26] that the security controls implemented within an information system are effective in their application. Assurance can be obtained in a variety of ways including: (i) actions taken by developers and implementers[27] of security controls in the design, development, and implementation techniques and methods; and (ii) actions taken by security control assessors during the testing and evaluation process to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Assurance considerations related to developers and implementers of security controls are addressed in this special publication. Assurance considerations related to assessors of security controls (including certification agents, evaluators, auditors, inspectors general) are addressed in NIST Special Publication 800-53A.

Appendix E describes the minimum assurance requirements for security controls listed in the low, moderate, and high baselines. For security controls in the low baseline, the emphasis is on the control being in place with the expectation that no obvious errors exist and that, as flaws are discovered, they are addressed in a timely manner. For security controls in the moderate baseline, the emphasis is on increasing grounds for confidence in control correctness. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer or control implementer incorporates, as part of the control, specific capabilities to increase grounds for confidence that the control meets its function or purpose. For security controls in the high baseline, the emphasis is on requiring within the control the capabilities that are needed to support ongoing, consistent operation of the control and to support continuous improvement in the control's effectiveness. There are additional assurance requirements available to developers and

[26] Confidence that the necessary security controls have been effectively implemented in organizational information systems provides a foundation for trust between organizations that depend upon the information processed, stored, or transmitted by those information systems.

[27] In this context, a developer/implementer is an individual or group of individuals responsible for the development or implementation of security controls for an information system. This may include, for example, hardware and software vendors providing the controls, contractors implementing the controls, or organizational personnel such as information system owners, information system security officers, system and network administrators, or other individuals with security responsibility for the information system.

implementers of security controls supplementing the minimum assurance requirements for the moderate and high baselines in order to protect against threats from highly skilled, highly motivated, and well-financed threat agents. This level of protection is necessary for those information systems where the organization is not willing to accept the risks associated with the type of threat agents cited above.

2.6 REVISIONS AND EXTENSIONS

The set of security controls listed in the control catalog represents the current state-of-the-practice safeguards and countermeasures for information systems. The security controls will be reviewed and revised periodically to reflect: (i) the experience gained from using the controls; (ii) the changing security requirements within organizations; (iii) emerging threats and attack methods; and (iv) the availability of new security technologies.[28] The controls in the control catalog are expected to change over time, as controls are eliminated or revised and new controls are added. The minimum security controls defined in the low, moderate, and high baselines are also expected to change over time as the level of security and due diligence for mitigating risks within organizations increases. In addition to the need for change, the need for stability will be addressed by requiring that proposed additions, deletions, or modifications to the catalog of security controls go through a rigorous public review process to obtain government and private sector feedback and to build consensus for the changes. A stable, yet flexible and technically rigorous set of security controls will be maintained in the control catalog.

[28] Currently, NIST plans to review and revise the security control catalog and security control baselines in Special Publication 800-53 on a biennial basis. The proposed modifications to security controls and security control baselines will be carefully weighed with each revision cycle, considering the desire for stability on one hand, and the need to respond to changing threats and vulnerabilities, new attack methods, new technologies, and the important objective of raising the foundational level of security over time.

CHAPTER THREE

THE PROCESS

SELECTION AND SPECIFICATION OF SECURITY CONTROLS

This chapter describes the process of selecting and specifying security controls for an information system.~~, including:~~

-(i)___-defining the organization's overall approach to managing risk; (see §3.1)

(ii)___-categorizing the system in accordance with FIPS 199;- (see §3.2)

(iii)__-selecting and tailoring the initial set of minimum (baseline) security controls;[29] (see §3.3)

-(iv)__-supplementing the tailored security control baseline as necessary based upon an organizational assessment of risk; and (see §3.4)

-(v)___-updating the controls as part of a comprehensive continuous monitoring process. (see §3.5)

3.1 MANAGING RISK

The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program that involves the management of risk—that is, the risk to the organization or to individuals associated with the operation of an information system. The management of risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system—the security controls necessary to protect individuals and the operations and assets of the organization. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, Executive Orders, directives, policies, standards, or regulations. The following activities related to managing risk (also known as the NIST *Risk Management Framework*) are paramount to an effective information security program and can be applied to both new and legacy information systems within the context of the system development life cycle and the Federal Enterprise Architecture—

3.1.1___***Categorize*** the information system and the information resident within that system based on a FIPS 199 impact analysis.

3.1.2___***Select*** an initial set of security controls (i.e., security control baseline from Appendix D) for the information system based on the FIPS 199 security categorization and the minimum security requirements defined in FIPS 200; apply tailoring guidance from Section 3.3 as appropriate, to obtain the control set used as the starting point for the assessment of risk associated with the use of the system.

3.1.3___***Supplement*** the initial set of tailored security controls based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances.[30]

[29] Tailoring guidance provides organizations with specific considerations on the applicability and implementation of individual security controls in the control baselines (see Section 3.3).

[30] NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, provides guidance

3.1.4 ***Document*** the agreed-upon set of security controls in the system security plan including the organization's rationale for any refinements or adjustments to the initial set of controls.[31]

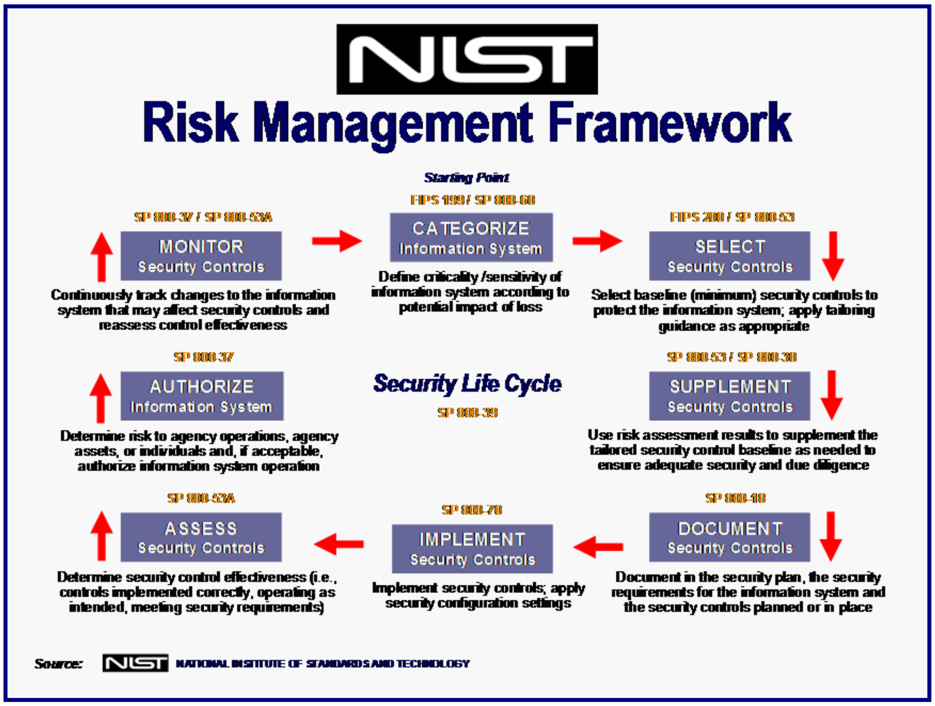
3.1.5 ***Implement*** the security controls in the information system. For legacy systems, some or all of the security controls selected may already be in place.

3.1.6 ***Assess*** the security controls using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.[32]

3.1.7 ***Authorize*** information system operation based upon a determination of the risk to organizational operations, organizational assets, or to individuals resulting from the operation of the information system and the decision that this risk is acceptable.[33]

3.1.8 ***Monitor*** and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis.

Figure 1 illustrates the specific activities in the NIST Risk Management Framework and the information security standards and guidance documents associated with each activity.


NIST
Risk Management Framework
Starting Point
FIPS 199 / SP 800-60
CATEGORIZE
Information System
Define criticality /sensitivity of information system according to potential impact of loss
FIPS 200 / SP 800-53
SELECT
Security Controls
Select baseline (minimum) security controls to protect the information system; apply tailoring guidance as appropriate
SP 800-53 / SP 800-30
SUPPLEMENT
Security Controls
Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence
SP 800-18
DOCUMENT
Security Controls
Document in the security plan, the security requirements for the information system and the security controls planned or in place
SP 800-70
IMPLEMENT
Security Controls
Implement security controls; apply security configuration settings
SP 800-53A
ASSESS
Security Controls
Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)
SP 800-37
AUTHORIZE
Information System
Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation
SP 800-37 / SP 800-53A
MONITOR
Security Controls
Continuously track changes to the information system that may affect security controls and reassess control effectiveness
Security Life Cycle
SP 800-39

Source: NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

FIGURE 1: THE RISK MANAGEMENT FRAMEWORK

on the assessment and mitigation of risk.

[31] NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, provides guidance on documenting information system security controls.

[32] NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft), April 2006, provides guidance for determining the effectiveness of security controls.

[33] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, provides guidance on the security authorization of information systems.

The remainder of this chapter focuses on several key activities in the Risk Management Framework—the FIPS 199 categorization, the initial selection and tailoring of security controls, supplementing the initial controls based on the organization's risk assessment, and updating the controls when necessary.

3.2 SECURITY CATEGORIZATION

FIPS 199, the mandatory ~~federal~~Federal security categorization standard, is predicated on a simple and well-established concept—determining appropriate priorities for organizational information systems and subsequently applying appropriate measures to adequately protect those systems. The security controls applied to a particular information system should be commensurate with the potential impact on organizational operations, organizational assets, or individuals should there be a loss of confidentiality, integrity, or availability. FIPS 199 requires organizations to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The potential impact values assigned to the respective security objectives are the highest values (i.e., high water mark) from among the security categories that have been determined for each type of information resident on those information systems.[34] The generalized format for expressing the security category (SC) of an information system is:

$$\textbf{SC}_{\text{ information system}} = \{(\textbf{confidentiality}, \textit{impact}), (\textbf{integrity}, \textit{impact}), (\textbf{availability}, \textit{impact})\},$$

where the acceptable values for potential impact are low, moderate, or high.

Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept is used to determine the impact level of the information system for the express purpose of selecting an initial set of security controls from one of the three security control baselines.[35] Thus, a *low-impact* system is defined as an information system in which all three of the security objectives are low. A *moderate-impact* system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a *high-impact* system is an information system in which at least one security objective is high.

[34] NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, provides guidance on the assignment of security categories to information systems.

[35] The high water mark concept is employed because there are significant dependencies among the security objectives of confidentiality, integrity, and availability. In most cases, a compromise in one security objective ultimately affects the other security objectives as well. Accordingly, the security controls in the control catalog are not categorized by security objective—rather, they are grouped into baselines to provide a general protection capability for classes of information systems based on impact level. The application of scoping guidance may allow selective security control baseline tailoring (see Section 3.3).

Implementation Tip

To determine the overall impact level of the information system:

- First, determine the different types of information that are processed, stored, or transmitted by the information system (e.g., financial sector oversight, inspections and auditing, official information dissemination, etc.). NIST Special Publication 800-60 provides guidance on a variety of information types commonly used by organizations.
- Second, using the impact levels in FIPS 199 and the recommendations of NIST Special Publication 800-60, categorize the confidentiality, integrity, and availability of each information type as low, moderate, or high impact.
- Third, determine the information system security categorization, that is, the highest impact level for each security objective (confidentiality, integrity, availability) from among the categorizations for the information types associated with the information system.
- Fourth, determine the overall impact level of the information system from the highest impact level among the three security objectives in the system security categorization.

3.3 SELECTING AND TAILORING THE INITIAL BASELINE

3.3.1 Choice of control baseline

Once the overall impact level of the information system is determined, an initial set of security controls can be selected from the corresponding low, moderate, or high baselines listed in Appendix D. Organizations have the flexibility to tailor the security control baselines in accordance with the terms and conditions set forth in this publication. Tailoring activities include:

a) ~~(i)~~ the application of appropriate *scoping guidance* to the initial baseline~~;~~ ;

b) ~~(ii)~~ the specification of *compensating security controls*, if needed; and

c) ~~(iii)~~ the specification of *organization-defined parameters* in the security controls, where allowed.

To achieve a cost-effective, risk-based approach to providing adequate information security organization-wide, security control baseline tailoring activities should be coordinated with and approved by appropriate organizational officials (e.g., chief information officers, senior agency information security officers, authorizing officials, or authorizing officials' designated representatives). Tailoring decisions should be documented in the security plan for the information system.[36]

3.3.~~1~~2 *Scoping Guidance*

Scoping guidance provides organizations with specific terms and conditions on the applicability and implementation of individual security controls in the security control baselines. There are several considerations, described below, that can potentially impact how the baseline security controls are applied by the organization:

a) Common security control-related considerations—

~~□~~Security controls designated by the organization as common controls are, in most cases, managed by an organizational entity other than the information system owner. Organizational decisions on which security controls are viewed as common controls may greatly affect the responsibilities of individual information system owners with regard to the implementation of controls in a particular baseline. Every control in a baseline must be fully addressed either by the organization or the information system owner.

b) Operational/environmental-related considerations—

~~□~~Security controls that are dependent on the nature of the operational environment are applicable only if the information system is employed in an environment necessitating the controls. For example, certain physical security controls may not be applicable to space-based information systems, and temperature and humidity controls may not be applicable to remote sensors that exist outside of the indoor facilities that contain information systems.

[36] It is important for organizations to document the decisions taken during the security control baseline tailoring process, providing a sound rationale for those decisions whenever possible. This documentation is essential when examining the overall security considerations for information systems with respect to potential mission and/or business case impact.

c) *Physical Infrastructure-related considerations—*

~~□~~Security controls that refer to organizational facilities (e.g., physical controls such as locks and guards, environmental controls for temperature, humidity, lighting, fire, and power) are applicable only to those sections of the facilities that directly provide protection to, support for, or are related to the information system (including its information technology assets such as electronic mail or web servers, server farms, data centers, networking nodes, boundary protection devices, and communications equipment).

d) *Public access-related considerations—*

~~□~~Security controls associated with public access information systems should be carefully considered and applied with discretion since some security controls from the specified control baselines (e.g., identification and authentication, personnel security controls) may not be applicable to users accessing information systems through public interfaces. For example, while the baseline controls require identification and authentication of organizational personnel that maintain and support information systems providing the public access services, the same controls might not be required for access to those information systems through public interfaces to obtain publicly available information. On the other hand, identification and authentication would be required for users accessing information systems through public interfaces in some instances, for example, to access/change their personal information.

e) *Technology-related considerations—*

i) 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 the information system.

ii) Security controls are applicable only to the components of the information system that provide or support the security capability addressed by the control and are sources of potential risk being mitigated by the control.[37] For example, when information system components are single-user, not networked, or only locally networked, one or more of these characteristics may provide appropriate rationale for not applying selected controls to that component.

iii) Security controls that can be either 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. In situations where automated mechanisms are not readily available, cost-effective, or technically feasible, compensating security controls, implemented through nonautomated mechanisms or procedures, should be used to satisfy specified security controls or control enhancements (see terms and conditions for applying compensating controls below).

f) *Policy/regulatory-related considerations—*

[37] For example, auditing controls would typically be applied to the components of an information system that provide or should provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the organization. Organizations should carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an organizational assessment of risk. While the tailoring guidance may support not applying a particular security control to a specific component (e.g., the audit example above), any residual risks associated with the absence of that control must still be addressed and mitigated as necessary to adequately protect the organization’s operations, assets, and individuals.

Security controls that address matters governed by applicable laws, Executive Orders, directives, policies, standards, or regulations (e.g., privacy impact assessments) are required only if the employment of those controls is consistent with the types of information and information systems covered by the applicable laws, Executive Orders, directives, policies, standards, or regulations.

~~f~~g) *Scalability-related considerations—*

~~□~~Security controls are scalable with regard to the extent and rigor of the control implementation. Scalability is guided by the FIPS 199 security categorization of the information system being protected. For example, a contingency plan for a FIPS 199 high-impact information system may be quite lengthy and contain a significant amount of implementation detail. In contrast, a contingency plan for a FIPS 199 low-impact information system may be considerably shorter and contain much less implementation detail. Organizations should use discretion in applying the security controls to information systems, giving consideration to the scalability factors in particular environments. This approach facilitates a cost-effective, risk-based approach to security control implementation that expends no more resources than necessary, yet achieves sufficient risk mitigation and adequate security.

~~g~~h) *Security objective-related considerations—*

~~□~~Security controls that uniquely support the confidentiality, integrity, or availability security objectives may be downgraded to the corresponding control in a lower baseline (or appropriately modified or eliminated if not defined in a lower baseline) if, and only if, the downgrading action: (i) is consistent with the FIPS 199 security categorization for the corresponding security objectives of confidentiality, integrity, or availability before moving to the high water mark;[38] (ii) is supported by an organizational assessment of risk; and (iii) does not affect the security-relevant information within the information system.[39] The following security controls are recommended candidates for downgrading: (i) confidentiality [AC-15, MA-3 (3), MP-2 (1), MP-3, MP-4, MP-5 (1) (2) (3), MP-6, PE-5, SC-4, SC-9]; (ii) integrity [SC-8]; and (iii) availability [CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, MA-6, PE-9, PE-10, PE-11, PE-13, PE-15, SC-6].[40]

[38] When applying the "high water mark" process in Section 3.2, some of the original FIPS 199 confidentiality, integrity, or availability security objectives may have been upgraded to a higher baseline of security controls. As part of this process, security controls that uniquely support the confidentiality, integrity, or availability security objectives may have been upgraded unnecessarily. Consequently, it is recommended that organizations consider appropriate and allowable downgrading actions to ensure cost-effective, risk-based application of security controls.

[39] Information that is security-relevant at the system level (e.g., password files, network routing tables, cryptographic key management information) is distinguished from user-level information within an information system. Certain security controls within an information system are used to support the security objectives of confidentiality and integrity for both user-level and system-level information. Caution should be exercised in downgrading confidentiality or integrity-related security controls to ensure that the downgrading action does not result in insufficient protection for the security-relevant information within the information system. Security-relevant information must be protected at the high water mark in order to achieve that level of protection for any of the security objectives related to user-level information.

[40] Certain security controls that are uniquely attributable to confidentiality, integrity, or availability that would ordinarily be considered as potential candidates for downgrading (e.g., AC-16, AU-10, CP-5, IA-7, PE-12, PE-14, PL-5, SC-5, SC-13, SC-14, SC-16) are eliminated from consideration because the controls are either selected for use in all baselines and have no enhancements that could be downgraded, or the controls are optional and not selected for use in any baseline. Organizations should exercise extreme caution when considering downgrading actions on any security controls that do not appear in the list in Section 3.3 to ensure that the downgrading action does not affect security objectives other than the objectives targeted for downgrading.

3.3.~~2~~3 Compensating Security Controls

With the diverse nature of today's information systems, organizations may find it necessary, on occasion, to specify and employ compensating security controls. A compensating security control is a management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provides equivalent or comparable protection for an information system.[41] A compensating control for an information system may be employed by an organization only under the following conditions:

(~~i~~a) the organization selects the compensating control from NIST Special Publication 800-53, or if an appropriate compensating control is not available in the security control catalog, the organization adopts a suitable compensating control;[42]

(~~ii~~b) the organization provides a complete and convincing rationale[43] for how the compensating control provides an equivalent security capability or level of protection for the information system and why the related baseline security control could not be employed; and

(~~iii~~c) the organization assesses and formally accepts the risk associated with employing the compensating control in the information system. The use of compensating security controls should be documented in the security plan for the information system and approved by the authorizing official.

3.3.~~3~~4 Organization-Defined Security Control Parameters

Security controls containing organization-defined parameters (i.e., assignment and/or selection operations) give organizations the flexibility to define selected portions of the controls to support specific organizational requirements or objectives (see AU-2 example in Section 2.1). After the application of the scoping guidance and the selection of compensating security controls, organizations should review the list of security controls for assignment and selection operations and determine appropriate organization-defined values for the identified parameters. Where specified, minimum and maximum values for organization-defined parameters should be adhered to unless more restrictive values are prescribed by applicable laws, Executive Orders, directives, policies, standards, or regulations or are indicated by the risk assessment in order to adequately mitigate risk. Organization-defined security control parameters should be documented in the security plan for the information system.

[41] More than one compensating control may be required to provide the equivalent or comparable protection for a particular security control in NIST Special Publication 800-53. For example, an organization with significant staff limitations may have difficulty in meeting the separation of duty security control but may employ compensating controls by strengthening the audit, accountability, and personnel security controls within the information system.

[42] Organizations should make every attempt to select compensating controls from the security control catalog in NIST Special Publication 800-53. Organization-defined compensating controls should be used only as a last resort when the security control catalog does not contain suitable compensating controls.

[43] The depth and rigor of the rationale provided should be scaled to the FIPS 199 impact level of the information system, with significantly less explanation needed for a low-impact system than for a high-impact system.

3.4 SUPPLEMENTING THE TAILORED BASELINE

3.4.1 Foundational tailored baseline

The tailored security control baseline should be viewed as the foundation or starting point in the selection of adequate security controls for an information system. The tailored baseline represents, for a particular class of information system (derived from the FIPS 199 security categorization and modified appropriately for local conditions), the starting point for determining the needed level of security *due diligence* to be demonstrated by an organization toward the protection of its operations and assets. As described in Section 3.1, the final determination of the appropriate set of security controls necessary to provide adequate security for an information system is a function of the organization's assessment of risk and what is required to sufficiently mitigate the risks to organizational operations, organizational assets, or individuals.[44]

3.4.2 Risk-based supplementation

In many cases, additional security controls or control enhancements will be needed to address specific threats to and vulnerabilities in an information system or to satisfy the requirements of applicable laws, Executive Orders, directives, policies, standards, or regulations. The risk assessment at this stage in the security control selection process provides important inputs to determine the sufficiency of the security controls in the tailored baseline—that is, the security controls needed to adequately protect the organization's operations (including mission, function, image, and reputation), the organization's assets, and individuals. Organizations are encouraged to make maximum use of the security control catalog to facilitate the process of enhancing security controls or adding controls to the tailored baseline. To assist in this process, the security control catalog in Appendix F contains numerous controls and control enhancements that are found only in higher-impact baselines or are not included in any of the baselines.

3.4.3 Supplementary use restrictions

There may be situations in which an organization discovers it is employing information technology beyond its ability to adequately protect critical and/or essential missions. That is, the organization cannot apply sufficient security controls within an information system to adequately reduce or mitigate mission risk. In those situations, an alternative strategy is needed to protect the mission from being impeded; a strategy that considers the mission risks that are being brought about by an aggressive use of information technology. Information system use restrictions provide an alternative method to reduce or mitigate risk, for example, when: (i) security controls cannot be implemented within technology and resource constraints; or (ii) security controls lack reasonable expectation of effectiveness against identified threat sources. Restrictions on the use of an information system are sometimes the only prudent or practical course of action to enable mission accomplishment in the face of determined adversaries.

The determination of required system use restrictions should be made by organizational officials having a vested interest in the accomplishment of organizational missions. These officials typically include, but are not limited to, the information system owner, mission owner, authorizing official, senior agency information security officer, and chief information officer. Examples of use restrictions include:

[44] The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system.

a) ~~(i)~~ limiting either the information an information system can process, store, or transmit or the manner in which a mission is automated;

b) ~~(ii)~~ prohibiting external information system access to critical organizational information by removing selected system components from the network (i.e., air gapping); and

~~1.~~c) ~~(iii)~~ prohibiting moderate- or high-impact information on an information system component to which the public has access, unless an explicit determination is made authorizing such access.

3.4.4 Record of decisions

It is important for organizations to document the decisions taken during the security control selection process, providing a sound rationale for those decisions whenever possible. This documentation is essential when examining the overall security considerations for information systems with respect to potential mission and/or business case impact. The resulting set of agreed-upon security controls along with the supporting rationale for control selection decisions and any information system use restrictions are documented in the security plan for the information system.

Figure 2 summarizes the security control selection process, including the tailoring of the initial security control baseline and any additional modifications to the baseline required based on the organization's assessment of risk.

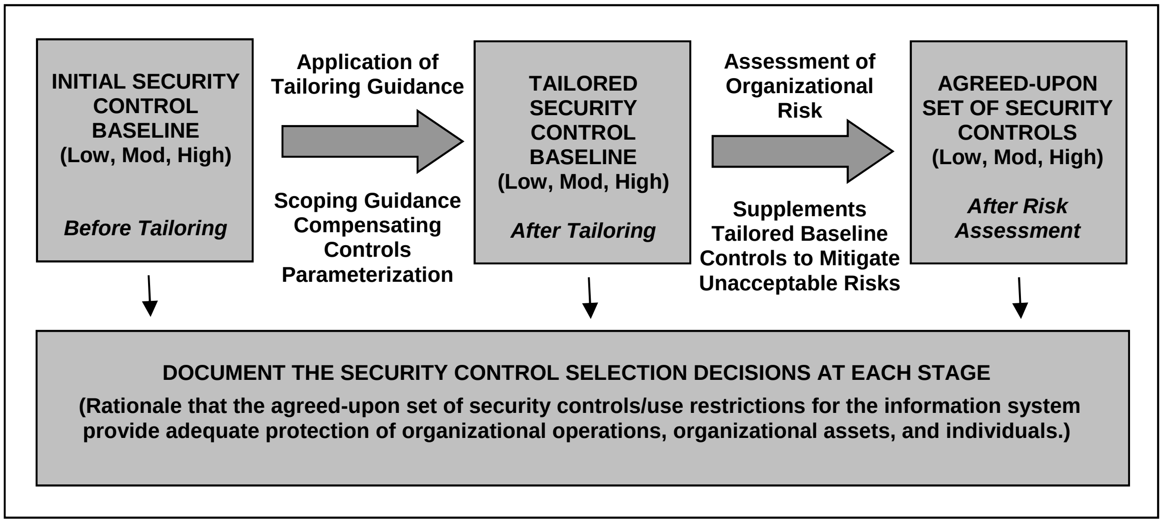

INITIAL SECURITY CONTROL BASELINE (Low, Mod, High)
Before Tailoring
Application of Tailoring Guidance
Scoping Guidance
Compensating Controls
Parameterization
TAILORED SECURITY CONTROL BASELINE (Low, Mod, High)
After Tailoring
Assessment of Organizational Risk
Supplements Tailored Baseline Controls to Mitigate Unacceptable Risks
AGREED-UPON SET OF SECURITY CONTROLS (Low, Mod, High)
After Risk Assessment
DOCUMENT THE SECURITY CONTROL SELECTION DECISIONS AT EACH STAGE
(Rationale that the agreed-upon set of security controls/use restrictions for the information system provide adequate protection of organizational operations, organizational assets, and individuals.)

FIGURE 2: SECURITY CONTROL SELECTION PROCESS

3.5 UPDATING SECURITY CONTROLS

3.5.1 Continuous monitoring of control applicability

As part of a comprehensive continuous monitoring program, organizations should initiate specific actions to determine if there is a need to update the current, agreed-upon set of security controls documented in the security plan and implemented within the information system. Specifically, the organization should revisit, on a regular basis, the risk management activities described in the Risk Management Framework in Section 3.1. Additionally, there are events which can trigger the immediate need to assess the security state of the information system and if required, update the current security controls. These events include, for example:

~~An incident results in a~~A breach to the information system, producing a loss of confidence in the confidentiality, integrity, or availability of information processed, stored, or transmitted by the system;

A newly identified, credible threat ~~exists~~ to the organization's operations or assets, or to individuals (due to the use of the information system supporting those operations, assets, or individuals) based on law enforcement information, intelligence information, or other credible sources of information; or

Significant changes to the configuration of the information system through the removal or addition of new or upgraded hardware, software, or firmware or changes in the operational environment potentially degrade the security state of the system.

3.5.2 Event-driven review of control applicability

When events such as those described above occur, organizations should at a minimum:[45]

[45] Organizations should determine the specific types of events that would trigger a modification to the security plan and changes to the security controls within the information system. The decision to commit resources in light of such events should be guided by an organizational assessment of risk to the organization's operations and assets, or to

a) *Reconfirm the criticality/sensitivity of the information system and the information processed, stored, and/or transmitted by that system.*

The organization should reexamine the FIPS 199 impact level of the information system to confirm the criticality/sensitivity of the system in supporting its mission operations or business case. The resulting impact on organizational operations, organizational assets, or individuals may provide new insights as to the overall importance of the system in allowing the organization to fulfill its mission responsibilities.

b) *Assess the current security state of the information system and reassess the current risk to organizational operations, organizational assets, and individuals.*

The organization should investigate the information system vulnerability (or vulnerabilities) exploited by the threat source (or that are potentially exploitable by a threat source) and the security controls currently implemented within the system as described in the security plan. The exploitation of an information system vulnerability (or vulnerabilities) by a threat source may be traced to one or more factors including but not limited to: (i) the failure of currently implemented security controls; (ii) missing security controls; (iii) insufficient strength of security controls; and/or (iv) an increase in the sophistication or capability of the threat source. Using the results from the assessment of the current security state, the organization should reassess the risks to organizational operations, organizational assets, or individuals arising from use of the information system.

c) *Plan for and initiate any necessary corrective actions.*

Based on the results of an updated risk assessment, the organization should determine what additional security controls and/or control enhancements may be necessary to address the vulnerability (or vulnerabilities) related to the event or what corrective actions may be needed to fix currently implemented controls deemed to be less than effective.

The security plan for the information system should then be updated to reflect these corrective actions. A Plan of Action and Milestones (POA&M) should be developed for any deficiencies noted that are not immediately corrected and for the implementation of any security control upgrades or additional controls. After the security controls or control upgrades have been implemented and any other noted deficiencies corrected, the controls should be assessed for effectiveness. The assessment determines if the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the organization's security policy.

d) *Consider reaccrediting the information system.*

Depending on the severity of the event, the impact on organizational operations, organizational assets, or individuals, and the extent of the corrective actions required to fix the identified deficiencies in the information system, the organization may need to consider reaccrediting the information system in accordance with the provisions of NIST Special Publication 800-37. The authorizing official makes the final determination on the need to reaccredit the information system in consultation with the system and mission owners, the senior agency information security officer, and the chief information officer. The authorizing official may choose to conduct an abbreviated reaccreditation focusing only on the affected components of the information system and the associated security controls and/or control enhancements which have been changed during the update. Authorizing officials should have sufficient information from the security certification process to initiate, with an appropriate

individuals, that would result if these modifications and changes are not made.

degree of confidence, the necessary corrective actions to adequately protect individuals and the organization’s operations and assets.

APPENDIX A

REFERENCES

LAWS, POLICIES, DIRECTIVES, REGULATIONS, MEMORANDA, STANDARDS, AND GUIDELINES

LEGISLATION

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
3. Paperwork Reduction Act (P.L. 104-13), May 1995.
4. USA PATRIOT Act (P.L. 107-56), October 2001.
5. Privacy Act of 1974 (P.L. 93-579), December 1974.

POLICIES, DIRECTIVES, REGULATIONS, AND MEMORANDA

6. Code of Federal Regulations, Title 5, *Administrative Personnel*, Section 731.106 *Designation of Public Trust Positions and Investigative Requirements*, (5 C.F.R. 731.106).
7. Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—Employees Responsible for the Management or Use of Federal Computer Systems, Section 930.301 through 930.305 (5 C.F.R 930.301-305).
8. Department of Defense Instruction 8500.2, *Information Assurance Implementation*, February 2003.
9. Director of Central Intelligence Directive 6/3 Policy, *Protecting Sensitive Compartmented Information within Information Systems*, June 1999.
10. Director of Central Intelligence Directive 6/3 Manual, *Protecting Sensitive Compartmented Information within Information Systems*, May 2000.
11. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.
12. Office of Management and Budget, Federal Enterprise Architecture Program Management Office, *Business Reference Model* (v2.0), June 2003.
13. Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001.
14. Office of Management and Budget Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting,* August 2003.
15. Office of Management and Budget Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 2003.
16. Office of Management and Budget Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 2003.
17. Office of Management and Budget Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2005.

18. Office of Management and Budget Memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 2006.

19. Office of Management and Budget Memorandum M-06-16, *Protection of Sensitive Information*, June 2006.

STANDARDS

20. International Organization for Standardization/International Electrotechnical Commission 27001, *Information security management system Requirements*, October 2005.

21. International Organization for Standardization/International Electrotechnical Commission ~~17799~~27002, *Code of Practice for information security management*, ~~June~~ April ~~2005~~2007 (Previously published as ISO/IEC 17799:2005, June 2005).

21a. *«shouldn't this be 21a, to avoid re-numbering all following refs, which may be employed by users of the existing published version?»* International Organization for Standardization/International Electrotechnical Commission 27006, *Requirements for bodies providing audit and certification of information security management*, February 2007

22. National Institute of Standards and Technology Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, May 2001.

23. National Institute of Standards and Technology Federal Information Processing Standards Publication 180-2, *Secure Hash Standard (SHS)*, August 2002.

24. National Institute of Standards and Technology Federal Information Processing Standards Publication 186-2, *Digital Signature Standard (DSS)*, January 2000.

25. National Institute of Standards and Technology Federal Information Processing Standards Publication 188, *Standard Security Labels for Information Transfer*, September 1994.

26. National Institute of Standards and Technology Federal Information Processing Standards Publication 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, September 1994.

27. National Institute of Standards and Technology Federal Information Processing Standards Publication 197, *Advanced Encryption Standard (AES)*, November 2001.

28. National Institute of Standards and Technology Federal Information Processing Standards Publication 198, *The Keyed-Hash Message Authentication Code (HMAC)*, March 2002.

29. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

30. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

31. National Institute of Standards and Technology Federal Information Processing Standards Publication 201-1, *Personal Identity Verification of Federal Employees and Contractors*, March 2006.

32. Committee for National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, June 2006.

33. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, *Protective Distribution Systems (PDS)*, December 1996.

GUIDELINES

34. National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

35. National Institute of Standards and Technology Special Publication 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network*, October 1995.

36. National Institute of Standards and Technology Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.

37. National Institute of Standards and Technology Special Publication 800-15, *Minimum Interoperability Specification for PKI Components (MISPC),* Version 1, September 1997.

38. National Institute of Standards and Technology Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998.

39. National Institute of Standards and Technology Special Publication 800-17, *Modes of Operation Validation System (MOVS): Requirements and Procedures*, February 1998.

40. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

41. National Institute of Standards and Technology Special Publication 800-19, *Mobile Agent Security*, October 1999.

42. National Institute of Standards and Technology Special Publication 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS)*: *Requirements and Procedures*, April 2000.

43. National Institute of Standards and Technology Special Publication 800-21-1, *Second Edition, Guideline for Implementing Cryptography in the Federal Government*, December 2005.

44. National Institute of Standards and Technology Special Publication 800-22, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, May 2001.

45. National Institute of Standards and Technology Special Publication 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000.

46. National Institute of Standards and Technology Special Publication 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does,* August 2000.

47. National Institute of Standards and Technology Special Publication 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000.

48. National Institute of Standards and Technology Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.

49. National Institute of Standards and Technology Special Publication 800-27, Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, June 2004.

50. National Institute of Standards and Technology Special Publication 800-28, *Guidelines on Active Content and Mobile Code*, October 2001.

51. National Institute of Standards and Technology Special Publication 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, June 2001.

52. National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

53. National Institute of Standards and Technology Special Publication 800-31, *Intrusion Detection Systems (IDS)*, November 2001.

54. National Institute of Standards and Technology Special Publication 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001.

55. National Institute of Standards and Technology Special Publication 800-33, *Underlying Technical Models for Information Technology Security*, December 2001.

56. National Institute of Standards and Technology Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.

57. National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services*, October 2003.

58. National Institute of Standards and Technology Special Publication 800-36, *Guide to Selecting Information Security Products*, October 2003.

59. National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

60. National Institute of Standards and Technology Special Publication 800-38A, *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*, December 2001.

61. National Institute of Standards and Technology Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005.

62. National Institute of Standards and Technology Special Publication 800-38C, *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*, May 2004.

63. National Institute of Standards and Technology Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication* (Draft), April 2006.

64. National Institute of Standards and Technology Special Publication 800-40, Version 2.0, *Creating a Patch and Vulnerability Management Program*, November 2005.

65. National Institute of Standards and Technology Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002.

66. National Institute of Standards and Technology Special Publication 800-42, *Guideline on Network Security Testing*, October 2003.

67. National Institute of Standards and Technology Special Publication 800-43, *Systems Administration Guidance for Windows 2000 Professional*, November 2002.

68. National Institute of Standards and Technology Special Publication 800-44, *Guidelines on Securing Public Web Servers*, September 2002.

69. National Institute of Standards and Technology Special Publication 800-45A (Draft), *Guidelines on Electronic Mail Security*, August 2006.

70. National Institute of Standards and Technology Special Publication 800-46, *Security for Telecommuting and Broadband Communications*, August 2002.

71. National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

72. National Institute of Standards and Technology Special Publication 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*, November 2002.

73. National Institute of Standards and Technology Special Publication 800-49, *Federal S/MIME V3 Client Profile*, November 2002.

74. National Institute of Standards and Technology Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003.

75. National Institute of Standards and Technology Special Publication 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*, September 2002.

76. National Institute of Standards and Technology Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, June 2005.

77. National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft), April 2006.

78. National Institute of Standards and Technology Special Publication 800-54, *Border Gateway Protocol Security* (Draft), September 2006.

79. National Institute of Standards and Technology Special Publication 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003.

80. National Institute of Standards and Technology Special Publication 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2006.

81. National Institute of Standards and Technology Special Publication 800-57, *Recommendation on Key Management*, August 2005.

82. National Institute of Standards and Technology Special Publication 800-58, *Security Considerations for Voice Over IP Systems*, January 2005.

83. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

84. National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

85. National Institute of Standards and Technology Special Publication 800-61, *Computer Security Incident Handling Guide*, January 2004.

86. National Institute of Standards and Technology Special Publication 800-63, Version 1.0.2, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Guidelines*, April 2006.

87. National Institute of Standards and Technology Special Publication 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle*, June 2004.

88. National Institute of Standards and Technology Special Publication 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005.

89. National Institute of Standards and Technology Special Publication 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005.

90. National Institute of Standards and Technology Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, May 2004.

91. National Institute of Standards and Technology Special Publication 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, October 2005.

92. National Institute of Standards and Technology Special Publication 800-69, *Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*, September 2006.

93. National Institute of Standards and Technology Special Publication 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*, May 2005.

94. National Institute of Standards and Technology Special Publication 800-72, *Guidelines on PDA Forensics*, November 2004.

95. National Institute of Standards and Technology Special Publication 800-73, Revision 1, *Interfaces for Personal Identity Verification*, April 2006.

96. National Institute of Standards and Technology Special Publication 800-76-1, *Biometric Data Specification for Personal Identity Verification* (Draft), September 2006.

97. National Institute of Standards and Technology Special Publication 800-77, *Guide to IPsec VPNs*, December 2005.

98. National Institute of Standards and Technology Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, April 2005.

99. National Institute of Standards and Technology Special Publication 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, July 2005.

100. National Institute of Standards and Technology Special Publication 800-81, *Secure Domain Name System (DNS) Deployment Guide*, May 2006.

101. National Institute of Standards and Technology Special Publication 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security* (Draft), September 2006.

102. National Institute of Standards and Technology Special Publication 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005.

103. National Institute of Standards and Technology Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006.

104. National Institute of Standards and Technology Special Publication 800-85A, *PIV Card Application and Middleware Interface Test Guidelines*, April 2006.

105. National Institute of Standards and Technology Special Publication 800-85B, *PIV Data Model Test Guidelines*, July 2006.

106. National Institute of Standards and Technology Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2006.

107. National Institute of Standards and Technology Special Publication 800-87, *Codes for the Identification of Federal and Federally-Assisted Organizations*, January 2006.

108. National Institute of Standards and Technology Special Publication 800-88, *Guidelines For Media Sanitization*, September 2006.

109. National Institute of Standards and Technology Special Publication 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications* November 2006.

110. National Institute of Standards and Technology Special Publication 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, June 2006.

111. National Institute of Standards and Technology Special Publication 800-92, *Guide to Computer Security Log Management*, September 2006.

112. National Institute of Standards and Technology Special Publication 800-94, *Guide to Intrusion Detection and Prevention (IDP) Systems* (Draft), August 2006.

113. National Institute of Standards and Technology Special Publication 800-95, *Guide to Secure Web Services* (Draft), August 2006.

114. National Institute of Standards and Technology Special Publication 800-96, *PIV Card / Reader Interoperability Guidelines*, September 2006.

115. National Institute of Standards and Technology Special Publication 800-97, *Guide to IEEE 802.11i: Establishing Robust Security Networks* (Draft), June 2006.

116. National Institute of Standards and Technology Special Publication 800-98, *Guidance for Securing Radio Frequency Identification (RFID) Systems* (Draft), September 2006.

117. National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.

118. National Institute of Standards and Technology Special Publication 800-101, *Guidelines on Cell Phone Forensics* (Draft), August 2006.

MISCELLANEOUS PUBLICATIONS

119. Department of Health and Human Services Centers for Medicare and Medicaid Services (CMS), *Core Set of Security Requirements*, February 2004.

120. Government Accountability Office, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6, January 1999.

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix B provides definitions for security terminology used within Special Publication 800-53. Unless specifically defined in this glossary, all terms used in this publication are consistent with the definitions contained in CNSS Instruction 4009, *National Information Assurance Glossary*.«is this still so? – two definitions have been added from 27001 (used in App. J)»

Accreditation
[FIPS 200, NIST SP 800-37]
The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. Also known as 'Authorization' (see NIST SP 800-37, footnote 6).

Accreditation Boundary
[NIST SP 800-37]
All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3.

Accrediting Authority
See Authorizing Official.

Adequate Security
[OMB Circular A-130, Appendix III]
Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Agency
See Executive Agency.

Authentication
[FIPS 200]
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authenticity
The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.

Authorize Processing
See Accreditation.

Authorizing Official
[FIPS 200, NIST SP 800-37]
Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority.

Authorization
Synonymous with 'Accreditation' (see NIST SP 800-37, footnote 6).

Availability
[44 U.S.C., Sec. 3542]
Ensuring timely and reliable access to and use of information.

Boundary Protection

Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).

Boundary Protection Device

A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) monitors and controls communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications. Boundary protection devices include such components as proxies, gateways, routers, firewalls, guards, and encrypted tunnels.

Certification
[FIPS 200, NIST SP 800-37]

A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Certification Agent
[NIST SP 800-37]

The individual, group, or organization responsible for conducting a security certification.

Certification Practice Statement

A statement of the practices that a Certification Authority employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in a certificate policy or requirements specified in a contract for services).

Chief Information Officer
[PL 104-106, Sec. 5125(b)]

Agency official responsible for:

(i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency;

(ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and

(iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

Commodity Service

An information system service (e.g., telecommunications service) provided by a commercial service provider typically to a large and diverse set of consumers. The organization acquiring and/or receiving the commodity service possesses limited visibility into the management structure and operations of the provider and while the organization may be able to negotiate service-level agreements, the organization is typically not in a position to require that the provider implement specific security controls.

Common Carrier

In a telecommunications context, a telecommunications company that holds itself out to the public for hire to provide communications transmission services. Note: In the United States, such companies are usually subject to regulation by ~~federal~~Federal and state regulatory commissions.

Common Security Control
[NIST SP 800-37]

Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.

Compensating Security Controls

The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.

Confidentiality
[44 U.S.C., Sec. 3542]

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Control
[CNSS Inst. 4009]

Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.

Countermeasures
[CNSS Inst. 4009]

Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.

Controlled Area

Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

Executive Agency
[41 U.S.C., Sec. 403]

An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.

External Information System (or Component)

An information system or component of an information system that is outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

External Information System Service

An information system service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system).

External Information System Service Provider

A provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.

Federal Enterprise Architecture
[FEA Program Management Office]

A business-based framework for governmentwide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the ~~federal~~Federal government to one that is citizen-centered, results-oriented, and market-based.

Federal Information System
[40 U.S.C., Sec. 11331]

An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

General Support System
[OMB Circular A-130, Appendix III]

An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

Guard (System)
[CNSS Inst. 4009, Adapted]

A mechanism limiting the exchange of information between information systems or subsystems.

High-Impact System
[FIPS 200]

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.

Incident
[FIPS 200]

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Industrial Control System

An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes.

Information
[FIPS 199]

An instance of an information type.

Information Owner
[CNSS Inst. 4009]

Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Resources
[44 U.S.C., Sec. 3502]

Information and related resources, such as personnel, equipment, funds, and information technology.

Information Security
[44 U.S.C., Sec. 3542]

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Management System (ISMS)
[ISO/IEC 27001:2005]

That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

NOTE: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

Information Security Policy
[CNSS Inst. 4009]

Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Information System
[44 U.S.C., Sec. 3502]
[OMB Circular A-130, Appendix III]

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Owner (or Program Manager)
[CNSS Inst. 4009, Adapted]

Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Information System Security Officer
[CNSS Inst. 4009, Adapted]

Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program.

Information Technology
[40 U.S.C., Sec. 1401]

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Information Type
[FIPS 199]

A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.

Integrity
[44 U.S.C., Sec. 3542]

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Label

See Security Label.

Line of Business

The following OMB-defined process areas common to virtually all ~~federal~~Federal agencies: Case Management, Financial Management, Grants Management, Human Resources Management, Federal Health Architecture, Information Systems Security, Budget Formulation and Execution, Geospatial, and IT Infrastructure.

Local Access

Access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network.

Low-Impact System
[FIPS 200]

An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.

Major Application
[OMB Circular A-130, Appendix III]

An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All ~~federal~~Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

Major Information System
[OMB Circular A-130]

An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

Malicious Code
[CNSS Inst. 4009]
[NIST SP 800-61]

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Malware

See Malicious Code.

Management Controls
[FIPS 200]

The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.

Media
[FIPS 200]

Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Media Access Control Address

A hardware address that uniquely identifies each component of an IEEE 802-based network. On networks that do not conform to the IEEE 802 standards but do conform to the OSI Reference Model, the node address is called the Data Link Control (DLC) address.

Media Sanitization
[NIST SP 800-88]

A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

Mobile Code

Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.

Mobile Code Technologies

Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).

Moderate-Impact System
[FIPS 200]

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high.

National Security Emergency Preparedness Telecommunications Services
[47 C.F.R., Part 64, App A]

Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States.

National Security Information

Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

National Security System
[44 U.S.C., Sec. 3542]

Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Non-repudiation
[CNSS Inst. 4009]

Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

Operational Controls
[FIPS 200]

The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).

Organization
[FIPS 200]

A ~~federal~~Federal agency or, as appropriate, any of its operational elements.

Plan of Action and Milestones
[OMB Memorandum 02-01]

A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Potential Impact
[FIPS 199]

The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS 199 low); (ii) a *serious* adverse effect (FIPS 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.

Privacy Impact Assessment
[OMB Memorandum 03-22]

An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privileged Function

A function executed on an information system involving the control, monitoring, or administration of the system.

Privileged User
[CNSS Inst. 4009]

Individual who has access to system control, monitoring, or administration functions (e.g., system administrator, information system security officer, maintainer, system programmer).

Protective Distribution System

Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.

Records

The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

Remote Access

Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).

Remote Maintenance

Maintenance activities conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet).

Risk
[FIPS 200]

The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Risk Assessment
[NIST SP 800-30, Adapted]

The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals arising through the operation of the information system. Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses, and considers mitigations provided by planned or in place security controls.

Risk Management
[FIPS 200]

The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

Safeguards
[CNSS Inst. 4009, Adapted]

Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Scoping Guidance

Provides organizations with specific policy/regulatory-related, technology-related, physical infrastructure-related, operational/environmental-related, public access-related, scalability-related, common security control-related, and security objective-related considerations on the applicability and implementation of individual security controls in the control baseline.

Security Category
[FIPS 199]

The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

Security Controls
[FIPS 199]

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Control Baseline
[FIPS 200]

The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.

Security Control Enhancements

Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.

Security Functions

The hardware, software, and firmware of the information system responsible for supporting and enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

Security Impact Analysis
[NIST SP 800-37]

The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system.

Security Incident

See Incident.

Security Label

Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein.

Security Objective
[FIPS 199]

Confidentiality, integrity, or availability.

Security Perimeter

See Accreditation Boundary.

Security Plan

See System Security Plan.

Security Requirements
[FIPS 200]

Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Senior Agency Information Security Officer
[44 U.S.C., Sec. 3544]

Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.

Spyware

Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

Statement of Applicability (SoA)
[ISO/IEC 27001:2005]

Documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS.

NOTE: Control objectives and controls are based on the results and conclusions of the risk assessment and risk treatment processes, legal or regulatory requirements, contractual obligations and the organization's business requirements for information security.

Subsystem

A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.

System

See Information System.

System-specific Security Control
[NIST SP 800-37]

A security control for an information system that has not been designated as a common security control.

System Security Plan
[NIST SP 800-18, Rev 1]

Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

Tailoring

The process by which a security control baseline selected in accordance with the FIPS 199 security categorization of the information system is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls, where allowed.

Tailored Security Control Baseline

Set of security controls resulting from the application of the tailoring guidance to the security control baseline.

Technical Controls
[FIPS 200]

The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Threat
[CNSS Inst. 4009, Adapted]
Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Threat Source
[FIPS 200]
The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.

Threat Assessment
[CNSS Inst. 4009]
Formal description and evaluation of threat to an information system.

Trusted Path
A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software.

User
[CNSS Inst. 4009]
Individual or (system) process authorized to access an information system.

Vulnerability
[CNSS Inst. 4009, Adapted]
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Assessment
[CNSS Inst. 4009]
Formal description and evaluation of the vulnerabilities in an information system.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

CFR	Code of Federal Regulations
CIO	Chief Information Officer
CNSS	Committee for National Security Systems
DCID	Director of Central Intelligence Directive
DNS	Domain Name System
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IEEE	Institute of Electrical and Electronics Engineers
ISMS	Information Security Management System
IPsec	Internet Protocol Security
NIST	National Institute of Standards and Technology
NSTISSI	National Security Telecommunications and Information System Security Instruction
OMB	Office of Management and Budget
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
POAM	Plan of Action and Milestones
SoA	Statement of Applicability
SP	Special Publication
TSP	Telecommunications Service Priority
VPN	Virtual Private Network
VoIP	Voice over Internet Protocol

APPENDIX D

MINIMUM SECURITY CONTROLS – SUMMARY

LOW-IMPACT, MODERATE-IMPACT, AND HIGH-IMPACT INFORMATION SYSTEMS

The following table lists the minimum security controls, or security control baselines, for low-impact, moderate-impact, and high-impact information systems. The three security control baselines are hierarchical in nature with regard to the security controls employed in those baselines.[46] If a security control is selected for one of the baselines, the family identifier and control number are listed in the appropriate column. If a control is not used in a particular baseline, the entry is marked "not selected." Control enhancements, when used to supplement basic security controls, are indicated by the number of the control enhancement. For example, an "IR-2 (1)" in the high baseline entry for the IR-2 security control indicates that the second control from the Incident Response family has been selected along with control enhancement (1). Some security controls and control enhancements in the security control catalog are not used in any of the baselines but are available for use by organizations if needed; for example, when the results of a risk assessment indicate the need for additional controls or control enhancements in order to adequately mitigate risks to individuals, the organization, or its assets. A complete description of security controls, supplemental guidance for the controls, and control enhancements is provided in Appendix F. A detailed listing of security controls and control enhancements for each control baseline is available at http://csrc.nist.gov/sec-cert.

«Suggestion – what about linking the first column control id to its catalog entry in Anx F, as a means for the user to quickly review it? And a link back??»

[46] The hierarchical nature applies to the security requirements of each control (i.e., the base control plus all of its enhancements) at the low-impact, moderate-impact, and high-impact level in that the control requirements at a particular impact level (e.g., AC-18 *Wireless Access Restrictions*—Moderate: AC-18 (1)) meets a stronger set of security requirements for that control than the next lower impact level of the same control (e.g., AC-18 *Wireless Access Restrictions*—Low: AC-18). Since the numerical designation of a control enhancement is neither indicative of the relative strength of the enhancement nor assumes any hierarchical relationship among enhancements, there are some controls (e.g., IA-2) that may not appear to satisfy the hierarchical nature of the security requirements of each control even though they do. For example, with IA-2 *User Identification and Authentication*, enhancement (1) is called out for the moderate baseline and enhancements (2) and (3) are called out for the high baseline. In this case, high [IA-2(2)(3)] is hierarchical to moderate [IA-2(1)] with regard to the security requirements being imposed.

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
Access Control				
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	AC-3	AC-3 (1)	AC-3 (1)
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6	AC-6
AC-7	Unsuccessful Login Attempts	AC-7	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8	AC-8
AC-9	Previous Logon Notification	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	Not Selected	Not Selected	AC-10
AC-11	Session Lock	Not Selected	AC-11	AC-11
AC-12	Session Termination	Not Selected	AC-12	AC-12 (1)
AC-13	Supervision and Review—Access Control	AC-13	AC-13 (1)	AC-13 (1)
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking	Not Selected	Not Selected	AC-15
AC-16	Automated Labeling	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access Restrictions	AC-18	AC-18 (1)	AC-18 (1) (2)
AC-19	Access Control for Portable and Mobile Devices	Not Selected	AC-19	AC-19
AC-20	Use of External Information Systems	AC-20	AC-20 (1)	AC-20 (1)
Awareness and Training				
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1
AT-2	Security Awareness	AT-2	AT-2	AT-2
AT-3	Security Training	AT-3	AT-3	AT-3
AT-4	Security Training Records	AT-4	AT-4	AT-4
AT-5	Contacts with Security Groups and Associations	Not Selected	Not Selected	Not Selected
Audit and Accountability				
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1
AU-2	Auditable Events	AU-2	AU-2 (3)	AU-2 (1) (2) (3)
AU-3	Content of Audit Records	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Monitoring, Analysis, and Reporting	Not Selected	AU-6 (2)	AU-6 (1) (2)
AU-7	Audit Reduction and Report Generation	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	AU-9	AU-9	AU-9

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	**MOD**	**HIGH**
AU-10	Non-repudiation	Not Selected	Not Selected	Not Selected
AU-11	Audit Record Retention	AU-11	AU-11	AU-11
	Certification, Accreditation, and Security Assessments			
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	CA-1	CA-1	CA-1
CA-2	Security Assessments	CA-2	CA-2	CA-2
CA-3	Information System Connections	CA-3	CA-3	CA-3
CA-4	Security Certification	CA-4	CA-4 (1)	CA-4 (1)
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5
CA-6	Security Accreditation	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7	CA-7	CA-7
	Configuration Management			
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (1)	CM-2 (1) (2)
CM-3	Configuration Change Control	Not Selected	CM-3	CM-3 (1)
CM-4	Monitoring Configuration Changes	Not Selected	CM-4	CM-4
CM-5	Access Restrictions for Change	Not Selected	CM-5	CM-5 (1)
CM-6	Configuration Settings	CM-6	CM-6	CM-6 (1)
CM-7	Least Functionality	Not Selected	CM-7	CM-7 (1)
CM-8	Information System Component Inventory	CM-8	CM-8 (1)	CM-8 (1) (2)
	Contingency Planning			
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1)	CP-2 (1) (2)
CP-3	Contingency Training	Not Selected	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing and Exercises	Not Selected	CP-4 (1)	CP-4 (1) (2)
CP-5	Contingency Plan Update	CP-5	CP-5	CP-5
CP-6	Alternate Storage Site	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1) (4)	CP-9 (1) (2) (3) (4)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10	CP-10 (1)
	Identification and Authentication			
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1
IA-2	User Identification and Authentication	IA-2	IA-2 (1)	IA-2 (2) (3)
IA-3	Device Identification and Authentication	Not Selected	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4	IA-4
IA-5	Authenticator Management	IA-5	IA-5	IA-5

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7
Incident Response				
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1
IR-2	Incident Response Training	Not Selected	IR-2	IR-2 (1)
IR-3	Incident Response Testing and Exercises	Not Selected	IR-3	IR-3 (1)
IR-4	Incident Handling	IR-4	IR-4 (1)	IR-4 (1)
IR-5	Incident Monitoring	Not Selected	IR-5	IR-5 (1)
IR-6	Incident Reporting	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7	IR-7 (1)	IR-7 (1)
Maintenance				
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	MA-2	MA-2 (1)	MA-2 (1) (2)
MA-3	Maintenance Tools	Not Selected	MA-3	MA-3 (1) (2) (3)
MA-4	Remote Maintenance	MA-4	MA-4 (1) (2)	MA-4 (1) (2) (3)
MA-5	Maintenance Personnel	MA-5	MA-5	MA-5
MA-6	Timely Maintenance	Not Selected	MA-6	MA-6
Media Protection				
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2 (1)	MP-2 (1)
MP-3	Media Labeling	Not Selected	Not Selected	MP-3
MP-4	Media Storage	Not Selected	MP-4	MP-4
MP-5	Media Transport	Not Selected	MP-5 (1) (2)	MP-5 (1) (2) (3)
MP-6	Media Sanitization and Disposal	MP-6	MP-6	MP-6 (1) (2)
Physical and Environmental Protection				
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2
PE-3	Physical Access Control	PE-3	PE-3	PE-3 (1)
PE-4	Access Control for Transmission Medium	Not Selected	Not Selected	PE-4
PE-5	Access Control for Display Medium	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	PE-6	PE-6 (1)	PE-6 (1) (2)
PE-7	Visitor Control	PE-7	PE-7 (1)	PE-7 (1)
PE-8	Access Records	PE-8	PE-8	PE-8 (1) (2)
PE-9	Power Equipment and Power Cabling	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	Not Selected	PE-10	PE-10 (1)
PE-11	Emergency Power	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	PE-12	PE-12	PE-12
PE-13	Fire Protection	PE-13	PE-13 (1) (2) (3)	PE-13 (1) (2) (3)

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-14	Temperature and Humidity Controls	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	Not Selected	PE-18	PE-18 (1)
PE-19	Information Leakage	Not Selected	Not Selected	Not Selected
Planning				
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1
PL-2	System Security Plan	PL-2	PL-2	PL-2
PL-3	System Security Plan Update	PL-3	PL-3	PL-3
PL-4	Rules of Behavior	PL-4	PL-4	PL-4
PL-5	Privacy Impact Assessment	PL-5	PL-5	PL-5
PL-6	Security-Related Activity Planning	Not Selected	PL-6	PL-6
Personnel Security				
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1
PS-2	Position Categorization	PS-2	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3	PS-3
PS-4	Personnel Termination	PS-4	PS-4	PS-4
PS-5	Personnel Transfer	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8
Risk Assessment				
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3
RA-4	Risk Assessment Update	RA-4	RA-4	RA-4
RA-5	Vulnerability Scanning	Not Selected	RA-5	RA-5 (1) (2)
System and Services Acquisition				
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2
SA-3	Life Cycle Support	SA-3	SA-3	SA-3
SA-4	Acquisitions	SA-4	SA-4 (1)	SA-4 (1)
SA-5	Information System Documentation	SA-5	SA-5 (1)	SA-5 (1) (2)
SA-6	Software Usage Restrictions	SA-6	SA-6	SA-6
SA-7	User Installed Software	SA-7	SA-7	SA-7
SA-8	Security Engineering Principles	Not Selected	SA-8	SA-8
SA-9	External Information System Services	SA-9	SA-9	SA-9

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-10	Developer Configuration Management	Not Selected	Not Selected	SA-10
SA-11	Developer Security Testing	Not Selected	SA-11	SA-11
System and Communications Protection				
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1
SC-2	Application Partitioning	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	Not Selected	Not Selected	SC-3
SC-4	Information Remnance	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5
SC-6	Resource Priority	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	SC-7	SC-7 (1) (2) (3) (4) (5)	SC-7 (1) (2) (3) (4) (5) (6)
SC-8	Transmission Integrity	Not Selected	SC-8	SC-8 (1)
SC-9	Transmission Confidentiality	Not Selected	SC-9	SC-9 (1)
SC-10	Network Disconnect	Not Selected	SC-10	SC-10
SC-11	Trusted Path	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	Not Selected	SC-12	SC-12
SC-13	Use of Cryptography	SC-13	SC-13	SC-13
SC-14	Public Access Protections	SC-14	SC-14	SC-14
SC-15	Collaborative Computing	Not Selected	SC-15	SC-15
SC-16	Transmission of Security Parameters	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17
SC-18	Mobile Code	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	Not Selected	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	Not Selected	Not Selected	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	Not Selected	SC-22	SC-22
SC-23	Session Authenticity	Not Selected	SC-23	SC-23
System and Information Integrity				
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	Information System Monitoring Tools and Techniques	Not Selected	SI-4 (4)	SI-4 (2) (4) (5)
SI-5	Security Alerts and Advisories	SI-5	SI-5	SI-5 (1)
SI-6	Security Functionality Verification	Not Selected	Not Selected	SI-6
SI-7	Software and Information Integrity	Not Selected	Not Selected	SI-7 (1) (2)

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-8	Spam Protection	Not Selected	SI-8	SI-8 (1)
SI-9	Information Input Restrictions	Not Selected	SI-9	SI-9
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	Not Selected	SI-10	SI-10
SI-11	Error Handling	Not Selected	SI-11	SI-11
SI-12	Information Output Handling and Retention	Not Selected	SI-12	SI-12

APPENDIX E

MINIMUM ASSURANCE REQUIREMENTS

LOW, MODERATE, AND HIGH BASELINE APPLICATIONS

The minimum assurance requirements for security controls described in the security control catalog are listed below. The assurance requirements are directed at the activities and actions that security control developers and implementers[47] define and apply to increase the level of confidence that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. The assurance requirements are applied on a control-by-control basis. The requirements are grouped by security control baseline (i.e., low, moderate, and high) since the requirements apply to each control within the respective baseline. Using a format similar to security controls, assurance requirements are followed by supplemental guidance that provides additional detail and explanation of how the requirements are to be applied. Bold~~ed~~ text indicates requirements that appear for the first time in a particular baseline.

Low Baseline

Assurance Requirement: **The security control is in effect and meets explicitly identified functional requirements in the control statement.**

Supplemental Guidance: For security controls in the low baseline, the focus is on the controls being in place with the expectation that no obvious errors exist and that, as flaws are discovered, they are addressed in a timely manner.

Moderate Baseline

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. **The control developer/implementer provides a description of the functional properties of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions supporting increased confidence that when the control is implemented, it will meet its required function or purpose. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.**

Supplemental Guidance: For security controls in the moderate baseline, the focus is on actions supporting increased confidence in the correct implementation and operation of the control. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer/implementer incorporates, as part of the control, specific capabilities and produces specific documentation supporting increased confidence that the control meets its required function or purpose. This documentation is also needed by assessors to analyze and test the functional properties of the control as part of the overall assessment of the control.

High Baseline

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties **and design/implementation** of the control with sufficient detail to permit analysis

[47] In this context, a developer/implementer is an individual or group of individuals responsible for the development or implementation of security controls for an information system. This may include, for example, hardware and software vendors providing the controls, contractors implementing the controls, or organizational personnel such as information system owners, information system security officers, system and network administrators, or other individuals with security responsibility for the information system.

and testing of the control (**including functional interfaces among control components)**. The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions supporting increased confidence that when the control is implemented, it will **continuously and consistently (i.e., across the information system)** meet its required function or purpose **and support improvement in the effectiveness of the control**. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.

Supplemental Guidance: For security controls in the high baseline, the focus is expanded to require, within the control, the capabilities that are needed to support ongoing consistent operation of the control and continuous improvement in the control's effectiveness. The developer/implementer is expected to expend significant effort on the design, development, implementation, and component/integration testing of the controls and to produce associated design and implementation documentation to support these activities. This documentation is also needed by assessors to analyze and test the internal components of the control as part of the overall assessment of the control.

Additional Requirements Enhancing the Moderate and High Baselines

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties and design/implementation of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, actions supporting increased confidence that when the control is implemented, it will continuously and consistently (i.e., across the information system) meet its required function or purpose and support improvement in the effectiveness of the control. These actions include requiring the development of records with structure and content suitable to facilitate making this determination. **The control is developed in a manner that supports a high degree of confidence that the control is complete, consistent, and correct.**

Supplemental Guidance: The additional high assurance requirements are intended to supplement the minimum assurance requirements for the moderate and high baselines, when appropriate, in order to protect against threats from highly skilled, highly motivated, and well-financed threat agents. This level of protection is necessary for those information systems where the organization is not willing to accept the risks associated with the type of threat agents cited above.

APPENDIX F

SECURITY CONTROL CATALOG

SECURITY CONTROLS, SUPPLEMENTAL GUIDANCE, AND CONTROL ENHANCEMENTS

The following catalog of security controls provides a range of safeguards and countermeasures for information systems. The security controls are organized into *families* for ease of use in the control selection and specification process. Each family contains security controls related to the security functionality of the family. A standardized, two-character identifier is assigned to uniquely identify each control family. To uniquely identify each control, a numeric identifier is appended to the family identifier to indicate the number of the control within the control family.

The security control structure consists of three key components: (i) a *control* section; (ii) a *supplemental guidance* section; and (iii) a *control enhancements* section. The control section provides a concise statement of the specific security capability needed to protect a particular aspect of an information system. The control statement describes specific security-related activities or actions to be carried out by the organization or by the information system. For some controls in the control catalog, a degree of flexibility is provided by allowing organizations to selectively define input values for certain parameters associated with the controls. This flexibility is achieved through the use of *assignment* and *selection* operations within the control.

The supplemental guidance section provides additional information related to a specific security control. Organizations are expected to apply the supplemental guidance as appropriate, when defining, developing, and implementing security controls. In certain instances, the supplemental guidance provides more detail concerning the control requirements or important considerations (and the needed flexibility) for implementing security controls in the context of an organization’s operational environment, specific mission requirements, or assessment of risk. In addition, applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance documents (e.g., OMB Circulars, FIPS, and NIST Special Publications) are listed in the supplemental guidance section, when appropriate, for the particular security control.[48]

The control enhancements section provides statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control. In both cases, the control enhancements are used in an information system requiring greater protection due to the potential impact of loss or when organizations seek additions to a basic control’s functionality based on the results of a risk assessment. Control enhancements are numbered sequentially within each control so the enhancements can be easily identified when selected to supplement the basic control. The numerical designation of a security control enhancement is used only to identify a particular enhancement within the control structure. The designation is neither indicative of the relative strength of the control enhancement nor assumes any hierarchical relationship among enhancements.

[48] NIST Special Publications listed in the supplemental guidance sections of security controls are assumed to refer to the most recent updates to those publications. For example, a reference to NIST Special Publication 800-18 refers to the Special Publication 800-18, Revision 1, which is the latest version of the security planning guideline.

Cautionary Note

The security controls described in this catalog should be employed in ~~federal~~Federal information systems in accordance with the risk management guidance provided in Chapter Three. This guidance includes the selection of minimum (baseline) security controls based upon the FIPS 199 security categorization of the information system and the tailoring of the minimum (baseline) security controls by: (i) applying appropriate scoping guidance; (ii) specifying compensating controls, if needed; and (iii) inserting organization-defined security control parameters, where allowed. Since the baseline security controls represent the minimum controls for low-impact, moderate-impact, and high-impact information systems, respectively, there are additional controls and control enhancements that appear in the catalog that are not used in any of the baselines. These additional security controls and control enhancements are available to organizations and can be used in supplementing the tailored baselines to achieve the needed level of protection in accordance with an organizational assessment of risk. Moreover, security controls and control enhancements contained in higher-level baselines can also be used by organizations to strengthen the level of protection provided in lower-level baselines, if deemed appropriate.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Supplemental Guidance: The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW AC-1	**MOD** AC-1	**HIGH** AC-1

AC-2 ACCOUNT MANAGEMENT

Control: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [*Assignment: organization-defined frequency, at least annually*].

Supplemental Guidance: Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know/need-to-share changes.

Control Enhancements:

(1) The organization employs automated mechanisms to support the management of information system accounts.

(2) The information system automatically terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].

(3) The information system automatically disables inactive accounts after [*Assignment: organization-defined time period*].

(4) The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.

LOW AC-2	**MOD** AC-2 (1) (2) (3) (4)	**HIGH** AC-2 (1) (2) (3) (4)

AC-3 ACCESS ENFORCEMENT

Control: The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.

Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant. Related security control: SC-13.

Control Enhancements:

(1) The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Enhancement Supplemental Guidance: Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

LOW AC-3	**MOD** AC-3 (1)	**HIGH** AC-3 (1)

AC-4 INFORMATION FLOW ENFORCEMENT

Control: The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability. Related security control: SC-7.

Control Enhancements:

(1) **The information system implements information flow control enforcement using explicit labels on information, source, and destination objects as a basis for flow control decisions.**

Enhancement Supplemental Guidance: Information flow control enforcement using explicit labels is used, for example, to control the release of certain types of information.

(2) **The information system implements information flow control enforcement using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.**

(3) **The information system implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions.**

LOW Not Selected	**MOD** AC-4	**HIGH** AC-4

AC-5 SEPARATION OF DUTIES

Control: The information system enforces separation of duties through assigned access authorizations.

Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.

Control Enhancements: None.

LOW Not Selected	**MOD** AC-5	**HIGH** AC-5

AC-6 LEAST PRIVILEGE

Control: The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Supplemental Guidance: The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.

Control Enhancements: None.

LOW Not Selected	**MOD** AC-6	**HIGH** AC-6

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

Control: The information system enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*] time period. The information system automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*], *delays next login prompt according to Assignment: organization-defined delay algorithm.*]] when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance: Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization.

Control Enhancements:

(1) The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

LOW AC-7	**MOD** AC-7	**HIGH** AC-7

AC-8 SYSTEM USE NOTIFICATION

Control: The information system displays an approved~~,~~ system-~~-~~use notification message before granting system access, informing potential users:

(i) that the user is accessing a U.S. Government information system;
(ii) that system usage may be monitored, recorded, and subject to audit;
(iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
~~-~~(iv) that use of the system indicates consent to monitoring and recording.

The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Supplemental Guidance: Privacy and security policies are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems: (i) the system use information is available and when appropriate, is displayed before granting access; (ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.

Control Enhancements: None.

LOW AC-8	**MOD** AC-8	**HIGH** AC-8

AC-9 PREVIOUS LOGON NOTIFICATION

Control: The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

Supplemental Guidance: None.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AC-10 CONCURRENT SESSION CONTROL

Control: The information system limits the number of concurrent sessions for any user to [*Assignment: organization-defined number of sessions*].

Supplemental Guidance: None.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** AC-10

AC-11 SESSION LOCK

Control: The information system prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

Supplemental Guidance: Users can directly initiate session lock mechanisms. A session lock is not a substitute for logging out of the information system. Organization-defined time periods of inactivity comply with ~~federal~~Federal policy; for example, in accordance with OMB Memorandum 06-16, the organization-defined time period is no greater than thirty minutes for remote access and portable devices.

Control Enhancements: None.

LOW Not Selected	**MOD** AC-11	**HIGH** AC-11

AC-12 SESSION TERMINATION

Control: The information system automatically terminates a remote session after [*Assignment: organization-defined time period*] of inactivity.

Supplemental Guidance: A remote session is initiated whenever an organizational information system is accessed by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).

Control Enhancements:

(1) Automatic session termination applies to local and remote sessions.

LOW Not Selected	**MOD** AC-12	**HIGH** AC-12 (1)

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

Control: The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.

Supplemental Guidance: The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently the activities of users with significant information system roles and responsibilities. The extent of the audit record reviews is based on the FIPS 199 impact level of the information system. For example, for low-impact systems, it is not intended that security logs be reviewed frequently for every workstation, but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records. NIST Special Publication 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the review of user activities.

LOW AC-13	**MOD** AC-13 (1)	**HIGH** AC-13 (1)

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control: The organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.

Supplemental Guidance: The organization allows limited user activity without identification and authentication for public websites or other publicly available information systems (e.g., individuals accessing a ~~federal~~Federal information system at http://www.firstgov.gov). Related security control: IA-2.

Control Enhancements:

(1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

LOW AC-14	**MOD** AC-14 (1)	**HIGH** AC-14 (1)

AC-15 AUTOMATED MARKING

Control: The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

Supplemental Guidance: Automated marking refers to markings employed on external media (e.g., hardcopy documents output from the information system). The markings used in external marking are distinguished from the labels used on internal data structures described in AC-16.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** AC-15

AC-16 AUTOMATED LABELING

Control: The information system appropriately labels information in storage, in process, and in transmission.

Supplemental Guidance: Automated labeling refers to labels employed on internal data structures (e.g., records, files) within the information system. Information labeling is accomplished in accordance with: (i) access control requirements; (ii) special dissemination, handling, or distribution instructions; or (iii) as otherwise required to enforce information system security policy.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AC-17 REMOTE ACCESS

Control: The organization authorizes, monitors, and controls all methods of remote access to the information system.

Supplemental Guidance: Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST Special Publication 800-63 provides guidance on remote electronic authentication. If the ~~federal~~ Federal Personal Identity Verification (PIV) credential is used as an identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST Special Publications 800-73 and 800-78. NIST Special Publication 800-77 provides guidance on IPsec-based virtual private networks. Related security control: IA-2.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

(2) The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.

(3) The organization controls all remote accesses through a limited number of managed access control points.

(4) The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

LOW AC-17	**MOD** AC-17 (1) (2) (3) (4)	**HIGH** AC-17 (1) (2) (3) (4)

AC-18 WIRELESS ACCESS RESTRICTIONS

Control: The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) authorizes, monitors, controls wireless access to the information system.

Supplemental Guidance: NIST Special Publications 800-48 and 800-97 provide guidance on wireless network security. NIST Special Publication 800-94 provides guidance on wireless intrusion detection and prevention.

Control Enhancements:

(1) The organization uses authentication and encryption to protect wireless access to the information system.

(2) The organization scans for unauthorized wireless access points [*Assignment: organization-defined frequency*] and takes appropriate action if such an access points are discovered.

Enhancement Supplemental Guidance: Organizations conduct a thorough scan for unauthorized wireless access points in facilities containing high-impact information systems. The scan is not limited to only those areas within the facility containing the high-impact information systems.

LOW AC-18	**MOD** AC-18 (1)	**HIGH** AC-18 (1) (2)

AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES

Control: The organization: (i) establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (ii) authorizes, monitors, and controls device access to organizational information systems.

Supplemental Guidance: Portable and mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are only allowed access to organizational information systems in accordance with organizational security policies and procedures. Security policies and procedures include device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), configuration management, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered in the media protection family. Related security controls: MP-4, MP-5.

Control Enhancements: None.

LOW Not Selected	**MOD** AC-19	**HIGH** AC-19

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

Control: The organization establishes terms and conditions for authorized individuals to: (i) access the information system from an external information system; and (ii) process, store, and/or transmit organization-controlled information using an external information system.

Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to, personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); information systems owned or controlled by non~~federal~~Federal governmental organizations; and ~~federal~~Federal information systems that are not owned by, operated by, or under the direct control of the organization.

Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system. This control does not apply to the use of external information systems to access organizational information systems and information that are intended for public access (e.g., individuals accessing ~~federal~~Federal information through public interfaces to organizational information systems). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Control Enhancements:

(1) The organization prohibits authorized individuals from using an external information system-to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization: (i) can verify the employment of required security controls on the external system as specified in the organization's information security policy and system security plan; or (ii) has approved information system connection or processing agreements with the organizational entity hosting the external information system.

LOW AC-20	**MOD** AC-20 (1)	**HIGH** AC-20 (1)

FAMILY: AWARENESS AND TRAINING **CLASS:** OPERATIONAL

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

Supplemental Guidance: The security awareness and training policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-16 and 800-50 provide guidance on security awareness and training. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW AT-1	**MOD** AT-1	**HIGH** AT-1

AT-2 SECURITY AWARENESS

Control: The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and [*Assignment: organization-defined frequency*~~,~~ *at least annually*] thereafter.

Supplemental Guidance: The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST Special Publication 800-50.

Control Enhancements: None.

LOW AT-2	**MOD** AT-2	**HIGH** AT-2

AT-3 SECURITY TRAINING

Control: The organization identifies personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.

Supplemental Guidance: The organization determines the appropriate content of security training based on the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides system managers, system and network administrators, and other personnel having access to system-level software, adequate technical training to perform their assigned duties. The organization's security training program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST Special Publication 800-50.

Control Enhancements: None.

LOW AT-3	**MOD** AT-3	**HIGH** AT-3

AT-4 SECURITY TRAINING RECORDS

Control: The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.

Supplemental Guidance: None.

Control Enhancements: None.

LOW AT-4	**MOD** AT-4	**HIGH** AT-4

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

Control: The organization establishes and maintains contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents.

Supplemental Guidance: To facilitate ongoing security education and training for organizational personnel in an environment of rapid technology changes and dynamic threats, the organization establishes and institutionalizes contacts with selected groups and associations within the security community. The groups and associations selected are in keeping with the organization's mission requirements. Information sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Supplemental Guidance: The audit and accountability policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW AU-1	**MOD** AU-1	**HIGH** AU-1

AU-2 AUDITABLE EVENTS

Control: The information system generates audit records for the following events: [*Assignment: organization-defined auditable events*].

Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverse the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST Special Publication 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The information system provides the capability to compile audit records from multiple components throughout the system into a system-wide (logical or physical), time-correlated audit trail.

(2) The information system provides the capability to manage the selection of events to be audited by individual components of the system.

(3) The organization periodically reviews and updates the list of organization-defined auditable events.

LOW AU-2	**MOD** AU-2 (3)	**HIGH** AU-2 (1) (2) (3)

AU-3 CONTENT OF AUDIT RECORDS

Control: The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

Supplemental Guidance: Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event. NIST Special Publication 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

(2) The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.

LOW AU-3	**MOD** AU-3 (1)	**HIGH** AU-3 (1) (2)

AU-4 AUDIT STORAGE CAPACITY

Control: The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

Supplemental Guidance: The organization provides sufficient audit storage capacity, taking into account the auditing to be performed and the online audit processing requirements. Related security controls: AU-2, AU-5, AU-6, AU-7, SI-4.

Control Enhancements: None.

LOW AU-4	**MOD** AU-4	**HIGH** AU-4

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system alerts appropriate organizational officials in the event of an audit processing failure and takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related security control: AU-4.

Control Enhancements:

(1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage of maximum audit record storage capacity*].

(2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].

LOW AU-5	**MOD** AU-5	**HIGH** AU-5 (1) (2)

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].

LOW Not Selected	**MOD** AU-6 (2)	**HIGH** AU-6 (1) (2)

AU-7 AUDIT REDUCTION AND REPORT GENERATION

Control: The information system provides an audit reduction and report generation capability.

Supplemental Guidance: Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.

Control Enhancements:

(1) The information system provides the capability to automatically process audit records for events of interest based upon selectable~~,~~ event criteria.

LOW Not Selected	**MOD** AU-7 (1)	**HIGH** AU-7 (1)

AU-8 TIME STAMPS

Control: The information system provides time stamps for use in audit record generation.

Supplemental Guidance: Time stamps (including date and time) of audit records are generated using internal system clocks.

Control Enhancements:

(1) The organization synchronizes internal information system clocks [*Assignment: organization-defined frequency*].

LOW AU-8	**MOD** AU-8 (1)	**HIGH** AU-8 (1)

AU-9 PROTECTION OF AUDIT INFORMATION

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Control Enhancements:

(1) The information system produces audit records on hardware-enforced, write-once media.

LOW AU-9	**MOD** AU-9	**HIGH** AU-9

AU-10 PERSONNEL ACCOUNTABILITY & NON-REPUDIATION

Control: The information system provides the capability to determine whether a given individual took a particular action.

Supplemental Guidance: Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects against later false claims by an individual of not having taken a specific action. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts, time stamps).

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AU-11 AUDIT RECORD RETENTION

Control: The organization retains audit records for [*Assignment: organization-defined time period*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Supplemental Guidance: The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. NIST Special Publication 800-61 provides guidance on computer security incident handling and audit record retention.

Control Enhancements: None.

LOW AU-11	**MOD** AU-11	**HIGH** AU-11

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS **CLASS:** MANAGEMENT

CA-1 CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT POLICIES AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.

Supplemental Guidance: The security assessment and certification and accreditation policies and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security assessment and certification and accreditation policies can be included as part of the general information security policy for the organization. Security assessment and certification and accreditation procedures can be developed for the security program in general, and for a particular information system, when required. The organization defines what constitutes a significant change to the information system to achieve consistent security reaccreditations. NIST Special Publication 800-53A provides guidance on security control assessments. NIST Special Publication 800-37 provides guidance on security certification and accreditation. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW CA-1	**MOD** CA-1	**HIGH** CA-1

CA-2 SECURITY ASSESSMENTS

Control: The organization conducts an assessment of the security controls in the information system [*Assignment: organization-defined frequency, at least annually*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Supplemental Guidance: This control is intended to support the FISMA requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be assessed with a frequency depending on risk, but no less than annually. The FISMA requirement for (at least) annual security control assessments should *not* be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security certification and accreditation process. To satisfy the annual FISMA assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) security certifications conducted as part of an information system accreditation or reaccreditation process (see CA-4); (ii) continuous monitoring activities (see CA-7); or (iii) testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed. Reuse of assessment information is critical in achieving a broad-based, cost-effective, and fully integrated security program capable of producing the needed evidence to determine the actual security status of the information system.

OMB does not require an annual assessment of *all* security controls employed in an organizational information system. In accordance with OMB policy, organizations must annually assess a subset of the security controls based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or confidence) that the organization must have in determining the effectiveness of the security controls in the information system. It is expected that the organization will assess all of the security controls in the information system during the three-year accreditation cycle. The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-4). NIST Special Publication 800-53A provides guidance on security control assessments to include reuse of existing assessment results. Related security controls: CA-4, CA-6, CA-7, SA-11.

Control Enhancements: None.

LOW CA-2	**MOD** CA-2	**HIGH** CA-2

CA-3 INFORMATION SYSTEM CONNECTIONS

Control: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.

Supplemental Guidance: Since FIPS 199 security categorizations apply to individual information systems, the organization carefully considers the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations also include information systems sharing the same networks. NIST Special Publication 800-47 provides guidance on connecting information systems. Related security controls: SC-7, SA-9.

Control Enhancements: None.

LOW CA-3	**MOD** CA-3	**HIGH** CA-3

CA-4 SECURITY CERTIFICATION

Control: The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Supplemental Guidance: A security certification is conducted by the organization in support of the OMB Circular A-130, Appendix III requirement for accrediting the information system. The security certification is a key factor in all security accreditation (i.e., authorization) decisions and is integrated into and spans the system development life cycle. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring (see CA-7). The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-2). NIST Special Publication 800-53A provides guidance on security control assessments. NIST Special Publication 800-37 provides guidance on security certification and accreditation. Related security controls: CA-2, CA-6, SA-11.

Control Enhancements:

(1) The organization employs an independent certification agent or certification team to conduct an assessment of the security controls in the information system.

Enhancement Supplemental Guidance: An independent certification agent or certification team is any individual or group capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the information system or to the determination of security control effectiveness. Independent security certification services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted certification services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the independence of the certification agent or certification team conducting the assessment of the security controls in the information system. The authorizing official decides on the required level of certifier independence based on the criticality and sensitivity of the information system and the ultimate risk to organizational operations and organizational assets, and to individuals. The authorizing official determines if the level of certifier independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision. In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the assessment of the security controls be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner or authorizing official, independence in the certification process can be achieved by ensuring the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, consistency, and veracity of the results. The authorizing official should consult with the Office of the Inspector General, the senior agency information security officer, and the chief information officer to fully discuss the implications of any decisions on certifier independence in the types of special circumstances described above.

LOW CA-4	**MOD** CA-4 (1)	**HIGH** CA-4 (1)

CA-5 PLAN OF ACTION AND MILESTONES

Control: The organization develops and updates [*Assignment: organization-defined frequency*], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

Supplemental Guidance: The plan of action and milestones is a key document in the security accreditation package developed for the authorizing official and is subject to ~~federal~~Federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. NIST Special Publication 800-37 provides guidance on the security certification and accreditation of information systems. NIST Special Publication 800-30 provides guidance on risk mitigation.

Control Enhancements: None.

LOW CA-5	**MOD** CA-5	**HIGH** CA-5

CA-6 SECURITY ACCREDITATION

Control: The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization [*Assignment: organization-defined frequency, at least every three years*] or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation.

Supplemental Guidance: OMB Circular A-130, Appendix III, establishes policy for security accreditations of ~~federal~~Federal information systems. The organization assesses the security controls employed within the information system before and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications. The security accreditation of an information system is not a static process. Through the employment of a comprehensive continuous monitoring process (the fourth and final phase of the certification and accreditation process), the critical information contained in the accreditation package (i.e., the system security plan, the security assessment report, and the plan of action and milestones) is updated on an ongoing basis providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system. To reduce the administrative burden of the three-year reaccreditation process, the authorizing official uses the results of the ongoing continuous monitoring process to the maximum extent possible as the basis for rendering a reaccreditation decision. NIST Special Publication 800-37 provides guidance on the security certification and accreditation of information systems. Related security controls: CA-2, CA-4, CA-7.

Control Enhancements: None.

LOW CA-6	**MOD** CA-6	**HIGH** CA-6

CA-7 CONTINUOUS MONITORING

Control: The organization monitors the security controls in the information system on an ongoing basis.

Supplemental Guidance: Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring. The selection of an appropriate subset of security controls is based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or grounds for confidence) that the organization must have in determining the effectiveness of the security controls in the information system. The organization establishes the selection criteria and subsequently selects a subset of the security controls employed within the information system for assessment. The organization also establishes the schedule for control monitoring to ensure adequate coverage is achieved. Those security controls that are volatile or critical to protecting the information system are assessed at least annually. All other controls are assessed at least once during the information system's three-year accreditation cycle. The organization can use the current year's assessment results obtained during continuous monitoring to meet the annual FISMA assessment requirement (see CA-2).

This control is closely related to and mutually supportive of the activities required in monitoring configuration changes to the information system. An effective continuous monitoring program results in ongoing updates to the information system security plan, the security assessment report, and the plan of action and milestones—the three principle documents in the security accreditation package. A rigorous and well executed continuous monitoring process significantly reduces the level of effort required for the reaccreditation of the information system. NIST Special Publication 800-37 provides guidance on the continuous monitoring process. NIST Special Publication 800-53A provides guidance on the assessment of security controls. Related security controls: CA-2, CA-4, CA-5, CA-6, CM-4.

Control Enhancements:

(1) The organization employs an independent certification agent or certification team to monitor the security controls in the information system on an ongoing basis.

Enhancement Supplemental Guidance: The organization can extend and maximize the value of the ongoing assessment of security controls during the continuous monitoring process by requiring an independent certification agent or team to assess all of the security controls during the information system's three-year accreditation cycle. Related security controls: CA-2, CA-4, CA-5, CA-6, CM-4.

LOW CA-7	**MOD** CA-7	**HIGH** CA-7

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

Supplemental Guidance: The configuration management policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW CM-1	**MOD** CM-1	**HIGH** CM-1

CM-2 BASELINE CONFIGURATION

Control: The organization develops, documents, and maintains a current baseline configuration of the information system.

Supplemental Guidance: This control establishes a baseline configuration for the information system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. The baseline configuration also provides the organization with a well-defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs/objectives. The baseline configuration of the information system is consistent with the Federal Enterprise Architecture. Related security controls: CM-6, CM-8.

Control Enhancements:

(1) The organization updates the baseline configuration of the information system as an integral part of information system component installations.

(2) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

LOW CM-2	**MOD** CM-2 (1)	**HIGH** CM-2 (1) (2)

CM-3 CONFIGURATION CHANGE CONTROL

Control: The organization authorizes, documents, and controls changes to the information system.

Supplemental Guidance: The organization manages configuration changes to the information system using an organizationally approved process (e.g., a chartered Configuration Control Board). Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications. Configuration change control includes changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers). The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. The approvals to implement a change to the information system include successful results from the security analysis of the change. The organization audits activities associated with configuration changes to the information system. Related security controls: CM-4, CM-6, SI-2.

Control Enhancements:

(1) **The organization employs automated mechanisms to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.**

LOW Not Selected	**MOD** CM-3	**HIGH** CM-3 (1)

CM-4 MONITORING CONFIGURATION CHANGES

Control: The organization monitors changes to the information system conducting security impact analyses to determine the effects of the changes.

Supplemental Guidance: Prior to change implementation, and as part of the change approval process, the organization analyzes changes to the information system for potential security impacts. After the information system is changed (including upgrades and modifications), the organization checks the security features to verify that the features are still functioning properly. The organization audits activities associated with configuration changes to the information system. Monitoring configuration changes and conducting security impact analyses are important elements with regard to the ongoing assessment of security controls in the information system. Related security control: CA-7.

Control Enhancements: None.

LOW Not Selected	**MOD** CM-4	**HIGH** CM-4

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control: The organization: (i) approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) generates, retains, and reviews records reflecting all such changes.

Supplemental Guidance: Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals obtain access to information system components for purposes of initiating changes, including upgrades, and modifications.

Control Enhancements:

(1) The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

LOW Not Selected	**MOD** CM-5	**HIGH** CM-5 (1)

CM-6 CONFIGURATION SETTINGS

Control: The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.

Supplemental Guidance: Configuration settings are the configurable parameters of the information technology products that compose the information system. Organizations monitor and control changes to the configuration settings in accordance with organizational policies and procedures. OMB FISMA reporting instructions provide guidance on configuration requirements for ~~federal~~Federal information systems. NIST Special Publication 800-70 provides guidance on producing and using configuration settings for information technology products employed in organizational information systems. Related security controls: CM-2, CM-3, SI-4.

Control Enhancements:

(1) The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.

LOW CM-6	**MOD** CM-6	**HIGH** CM-6 (1)

CM-7 LEAST FUNCTIONALITY

Control: The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services*].

Supplemental Guidance: Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component. Where feasible, the organization limits component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing).

Control Enhancements:

(1) The organization reviews the information system [*Assignment: organization-defined frequency*], to identify and eliminate unnecessary functions, ports, protocols, and/or services.

LOW Not Selected	**MOD** CM-7	**HIGH** CM-7 (1)

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Control: The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.

Supplemental Guidance: The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system. Related security controls: CM-2, CM-6.

Control Enhancements:

(1) The organization updates the inventory of information system components as an integral part of component installations.

(2) The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

LOW CM-8	**MOD** CM-8 (1)	**HIGH** CM-8 (1) (2)

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

Supplemental Guidance: The contingency planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-34 provides guidance on contingency planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW CP-1	**MOD** CP-1	**HIGH** CP-1

CP-2 CONTINGENCY PLAN

Control: The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization coordinates contingency plan development with organizational elements responsible for related plans.

Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.

(2) The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.

LOW CP-2	**MOD** CP-2 (1)	**HIGH** CP-2 (1) (2)

CP-3 CONTINGENCY TRAINING

Control: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency, at least annually*].

Supplemental Guidance: None.

Control Enhancements:

(1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.

LOW Not Selected	**MOD** CP-3	**HIGH** CP-3 (1)

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

Control: The organization: (i) tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan; and (ii) reviews the contingency plan test/exercise results and initiates corrective actions.

Supplemental Guidance: There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, functional/tabletop exercises). The depth and rigor of contingency plan testing and/or exercises increases with the FIPS 199 impact level of the information system. Contingency plan testing and/or exercises also include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan. NIST Special Publication 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.

Control Enhancements:

(1) The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.

(2) The organization tests/exercises 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.

(3) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the contingency plan by providing more complete coverage of contingency issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the information system and supported missions.

LOW Not Selected	**MOD** CP-4 (1)	**HIGH** CP-4 (1) (2)

CP-5 CONTINGENCY PLAN UPDATE

Control: The organization reviews the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

Supplemental Guidance: Organizational changes include changes in mission, functions, or business processes supported by the information system. The organization communicates changes to appropriate organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).

Control Enhancements: None.

LOW CP-5	**MOD** CP-5	**HIGH** CP-5

CP-6 ALTERNATE STORAGE SITE

Control: The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.

Supplemental Guidance: The frequency of information system backups and the transfer rate of backup information to the alternate storage site (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives.

Control Enhancements:

(1) The organization identifies an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards.

(2) The organization configures the alternate storage site to facilitate timely and effective recovery operations.

(3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

LOW Not Selected	**MOD** CP-6 (1) (3)	**HIGH** CP-6 (1) (2) (3)

CP-7 ALTERNATE PROCESSING SITE

Control: The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [*Assignment: organization-defined time period*] when the primary processing capabilities are unavailable.

Supplemental Guidance: Equipment and supplies required to resume operations within the organization-defined time period are either available at the alternate site or contracts are in place to support delivery to the site. Timeframes to resume information system operations are consistent with organization-established recovery time objectives.

Control Enhancements:

(1) The organization identifies an alternate processing site that is geographically separated from the primary processing site so as not to be susceptible to the same hazards.

(2) The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

(3) The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

(4) The organization fully configures the alternate processing site so that it is ready to be used as the operational site supporting a minimum required operational capability.

LOW Not Selected	**MOD** CP-7 (1) (2) (3)	**HIGH** CP-7 (1) (2) (3) (4)

CP-8 TELECOMMUNICATIONS SERVICES

Control: The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable.

Supplemental Guidance: In the event that the primary and/or alternate telecommunications services are provided by a common carrier, the organization requests Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness (see http://tsp.ncs.gov for a full explanation of the TSP program).

Control Enhancements:

(1) The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

(2) The organization obtains alternate telecommunications services that do not share a single point of failure with primary telecommunications services.

(3) The organization obtains alternate telecommunications service providers that are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.

(4) The organization requires primary and alternate telecommunications service providers to have adequate contingency plans.

LOW Not Selected	**MOD** CP-8 (1) (2)	**HIGH** CP-8 (1) (2) (3) (4)

CP-9 INFORMATION SYSTEM BACKUP

Control: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [*Assignment: organization-defined frequency*] and protects backup information at the storage location.

Supplemental Guidance: The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives. While integrity and availability are the primary concerns for system backup information, protecting backup information from unauthorized disclosure is also an important consideration depending on the type of information residing on the backup media and the FIPS 199 impact level. An organizational assessment of risk guides the use of encryption for backup information. The protection of system backup information while in transit is beyond the scope of this control. Related security controls: MP-4, MP-5.

Control Enhancements:

(1) **The organization tests backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.**

(2) **The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.**

(3) **The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.**

(4) **The organization protects system backup information from unauthorized modification.**

Enhancement Supplemental Guidance: The organization employs appropriate mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of information system backups. Protecting the confidentiality of system backup information is beyond the scope of this control. Related security controls: MP-4, MP-5.

LOW CP-9	**MOD** CP-9 (1) (4)	**HIGH** CP-9 (1) (2) (3) (4)

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.

Supplemental Guidance: Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested.

Control Enhancements:

(1) **The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.**

LOW CP-10	**MOD** CP-10	**HIGH** CP-10 (1)

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Supplemental Guidance: The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and Special Publications 800-73, 800-76, and 800-78; and (ii) other applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. NIST Special Publication 800-63 provides guidance on remote electronic authentication.

Control Enhancements: None.

LOW IA-1	**MOD** IA-1	**HIGH** IA-1

IA-2 USER IDENTIFICATION AND AUTHENTICATION

Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users).

Supplemental Guidance: Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. NIST Special Publication 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms. For purposes of this control, the guidance provided in Special Publication 800-63 is applied to both local and remote access to information systems. Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Local access is any access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network. Unless a more stringent control enhancement is specified, authentication for both local and remote information system access is NIST Special Publication 800-63 level 1 compliant. FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of ~~federal~~Federal employees and contractors. In addition to identifying and authenticating users at the information system level (i.e., at system logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

In accordance with OMB policy and E-Authentication E-Government initiative, authentication of public users accessing ~~federal~~Federal information systems may also be required to protect nonpublic or privacy-related information. The e-authentication risk assessment conducted in accordance with OMB Memorandum 04-04 is used in determining the NIST Special Publication 800-63 compliance requirements for such accesses with regard to the IA-2 control and its enhancements. Scalability, practicality, and security issues are simultaneously considered in balancing the need to ensure ease of use for public access to such information and information systems with the need to protect organizational operations, organizational assets, and individuals. Related security controls: AC-14, AC-17.

Control Enhancements:

(1) **The information system employs multifactor authentication for *remote* system access that is NIST Special Publication 800-63 [*Selection: organization-defined level 3, level 3 using a hardware authentication device, or level 4*] compliant.**

(2) **The information system employs multifactor authentication for *local* system access that is NIST Special Publication 800-63 [*Selection: organization-defined level 3 or level 4*] compliant.**

(3) **The information system employs multifactor authentication for *remote* system access that is NIST Special Publication 800-63 level 4 compliant.**

LOW IA-2	**MOD** IA-2 (1)	**HIGH** IA-2 (2) (3)

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: The information system identifies and authenticates specific devices before establishing a connection.

Supplemental Guidance: The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the FIPS 199 security categorization of the information system with higher impact levels requiring stronger authentication.

Control Enhancements: None.

LOW Not Selected	**MOD** IA-3	**HIGH** IA-3

IA-4 IDENTIFIER MANAGEMENT

Control: The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) issuing the user identifier to the intended party; (v) disabling the user identifier after [*Assignment: organization-defined time period*] of inactivity; and (vi) archiving user identifiers.

Supplemental Guidance: Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts). FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of ~~federal~~Federal employees and contractors.

Control Enhancements: None.

LOW IA-4	**MOD** IA-4	**HIGH** IA-4

IA-5 AUTHENTICATOR MANAGEMENT

Control: The organization manages information system authenticators*«RGW: where does this word come from? It is not defined and I'm not sure it is common parlance (or maybe that's my language problem ;-). Wouldn't 'credential' be preferable? In fact, surely the device is not the authenticator, it is a credential, which in combination with other factors allows the identity to be authenticated, hence the 'authenticator' is the function / process of verifying the credential and those other factors.»* by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.

Supplemental Guidance: Information system authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users should take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the information system: (i) validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account. In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing ~~federal~~Federal information systems (and associated authenticator management) may also be required to protect nonpublic or privacy-related information. FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of ~~federal~~Federal employees and contractors. NIST Special Publication 800-63 provides guidance on remote electronic authentication.

Control Enhancements: None.

LOW IA-5	**MOD** IA-5	**HIGH** IA-5

IA-6 AUTHENTICATOR FEEDBACK

Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Supplemental Guidance: The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.

Control Enhancements: None.

LOW IA-6	**MOD** IA-6	**HIGH** IA-6

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control: The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

Supplemental Guidance: The applicable ~~federal~~Federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.

Control Enhancements: None.

LOW IA-7	**MOD** IA-7	**HIGH** IA-7

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Supplemental Guidance: The incident response policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. NIST Special Publication 800-61 provides guidance on incident handling and reporting. NIST Special Publication 800-83 provides guidance on malware incident handling and prevention.

Control Enhancements: None.

LOW IR-1	**MOD** IR-1	**HIGH** IR-1

IR-2 INCIDENT RESPONSE TRAINING

Control: The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency, at least annually*].

Supplemental Guidance: None.

Control Enhancements:

(1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.

LOW Not Selected	**MOD** IR-2	**HIGH** IR-2 (1)

IR-3 INCIDENT RESPONSE TESTING AND EXERCISES

Control: The organization tests and/or exercises the incident response capability for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: organization-defined tests and/or exercises*] to determine the incident response effectiveness and documents the results.

Supplemental Guidance: NIST Special Publication 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.

Control Enhancements:

(1) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability.

Enhancement Supplemental Guidance: Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the capability by providing more complete coverage of incident response issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the response capability.

LOW Not Selected	**MOD** IR-3	**HIGH** IR-3 (1)

IR-4 INCIDENT HANDLING

Control: The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

Supplemental Guidance: Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly. Related security controls: AU-6, PE-6.

Control Enhancements:

(1) The organization employs automated mechanisms to support the incident handling process.

LOW IR-4	**MOD** IR-4 (1)	**HIGH** IR-4 (1)

IR-5 INCIDENT MONITORING

Control: The organization tracks and documents information system security incidents on an ongoing basis.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

LOW Not Selected	**MOD** IR-5	**HIGH** IR-5 (1)

IR-6 INCIDENT REPORTING

Control: The organization promptly reports incident information to appropriate authorities.

Supplemental Guidance: The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Organizational officials report cyber security incidents to the United States Computer Emergency Readiness Team (US-CERT) at http://www.us-cert.gov within the specified timeframe designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. In addition to incident information, weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents. NIST Special Publication 800-61 provides guidance on incident reporting.

Control Enhancements:

(1) The organization employs automated mechanisms to assist in the reporting of security incidents.

LOW IR-6	**MOD** IR-6 (1)	**HIGH** IR-6 (1)

IR-7 INCIDENT RESPONSE ASSISTANCE

Control: The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.

Supplemental Guidance: Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required.

Control Enhancements:

(1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.

LOW IR-7	**MOD** IR-7 (1)	**HIGH** IR-7 (1)

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.

Supplemental Guidance: The information system maintenance policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW MA-1	**MOD** MA-1	**HIGH** MA-1

MA-2 CONTROLLED MAINTENANCE

Control: The organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

Supplemental Guidance: All maintenance activities to include routine, scheduled maintenance and repairs are controlled; whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. Organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures. After maintenance is performed on the information system, the organization checks all potentially impacted security controls to verify that the controls are still functioning properly.

Control Enhancements:

(1) The organization maintains maintenance records for the information system that include: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).

(2) The organization employs automated mechanisms to schedule and conduct maintenance as required, and to create up-to date, accurate, complete, and available records of all maintenance actions, both needed and completed.

LOW MA-2	**MOD** MA-2 (1)	**HIGH** MA-2 (1) (2)

MA-3 MAINTENANCE TOOLS

Control: The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.

Supplemental Guidance: The intent of this control is to address hardware and software brought into the information system specifically for diagnostic/repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control.

Control Enhancements:

(1) The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.

Enhancement Supplemental Guidance: Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system.

(2) The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.

(3) The organization checks all maintenance equipment with the capability of retaining information so that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.

(4) The organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.

LOW Not Selected	**MOD** MA-3	**HIGH** MA-3 (1) (2) (3)

MA-4 REMOTE MAINTENANCE

Control: The organization authorizes, monitors, and controls any remotely executed maintenance and diagnostic activities, if employed.

Supplemental Guidance: Remote maintenance and diagnostic activities are conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). The use of remote maintenance and diagnostic tools is consistent with organizational policy and documented in the security plan for the information system. The organization maintains records for all remote maintenance and diagnostic activities. Other techniques and/or controls to consider for improving the security of remote maintenance include: (i) encryption and decryption of communications; (ii) strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST Special Publication 800-63; and (iii) remote disconnect verification. When remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections invoked in the performance of that activity. If password-based authentication is used to accomplish remote maintenance, the organization changes the passwords following each remote maintenance service. NIST Special Publication 800-88 provides guidance on media sanitization. The National Security Agency provides a listing of approved media sanitization products at http://www.nsa.gov/ia/government/mdg.cfm. Related security controls: IA-2, MP-6.

Control Enhancements:

(1) The organization audits all remote maintenance and diagnostic sessions and appropriate organizational personnel review the maintenance records of the remote sessions.

(2) The organization addresses the installation and use of remote maintenance and diagnostic links in the security plan for the information system.

(3) The organization does not allow remote maintenance or diagnostic services to be performed by a provider that does not implement for its own information system, a level of security at least as high as that implemented on the system being serviced, unless the component being serviced is removed from the information system and sanitized (with regard to organizational information) before the service begins and also sanitized (with regard to potentially malicious software) after the service is performed and before being reconnected to the information system.

LOW MA-4	**MOD** MA-4 (1) (2)	**HIGH** MA-4 (1) (2) (3)

MA-5 MAINTENANCE PERSONNEL

Control: The organization allows only authorized personnel to perform maintenance on the information system.

Supplemental Guidance: Maintenance personnel (whether performing maintenance locally or remotely) have appropriate access authorizations to the information system when maintenance activities allow access to organizational information or could result in a future compromise of confidentiality, integrity, or availability. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system.

Control Enhancements: None.

LOW MA-5	**MOD** MA-5	**HIGH** MA-5

MA-6 TIMELY MAINTENANCE

Control: The organization obtains maintenance support and spare parts for [*Assignment: organization-defined list of key information system components*] within [*Assignment: organization-defined time period*] of failure.

Supplemental Guidance: None.

Control Enhancements: None.

LOW Not Selected	**MOD** MA-6	**HIGH** MA-6

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

Supplemental Guidance: The media protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW MP-1	**MOD** MP-1	**HIGH** MP-1

MP-2 MEDIA ACCESS

Control: The organization restricts access to information system media to authorized individuals.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones).

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection.

Control Enhancements:

(1) The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

Enhancement Supplemental Guidance: This control enhancement is primarily applicable to designated media storage areas within an organization where a significant volume of media is stored and is not intended to apply to every location where some media is stored (e.g., in individual offices).

LOW MP-2	**MOD** MP-2 (1)	**HIGH** MP-2 (1)

MP-3 MEDIA LABELING

Control: The organization: (i) affixes external labels to removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and (ii) exempts [*Assignment: organization-defined list of media types or hardware components*] from labeling so long as they remain within [*Assignment: organization-defined protected environment*].

Supplemental Guidance: An organizational assessment of risk guides the selection of media requiring labeling. Organizations document in policy and procedures, the media requiring labeling and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, labeling is not required for media containing information determined by the organization to be in the public domain or to be publicly releasable.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** MP-3

MP-4 MEDIA STORAGE

Control: The organization physically controls and securely stores information system media within controlled areas.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Organizations document in policy and procedures, the media requiring physical protection and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection. The organization protects information system media identified by the organization until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

As part of a defense-in-depth protection strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. FIPS 199 security categorization guides the selection of appropriate candidates for secondary storage encryption. The organization implements effective cryptographic key management in support of secondary storage encryption and provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users. NIST Special Publications 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Related security controls: CP-9, RA-2.

Control Enhancements: None.

LOW Not Selected	**MOD** MP-4	**HIGH** MP-4

MP-5 MEDIA TRANSPORT

Control: The organization protects and controls information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. An organizational assessment of risk guides the selection of media and associated information contained on that media requiring protection during transport. Organizations document in policy and procedures, the media requiring protection during transport and the specific measures taken to protect such transported media. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. An organizational assessment of risk also guides the selection and use of appropriate storage containers for transporting non-digital media. Authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service).

Control Enhancements:

(1) The organization protects digital and non-digital media during transport outside of controlled areas using [*Assignment: organization-defined security measures, e.g., locked container, cryptography*].

Enhancement Supplemental Guidance: Physical and technical security measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FIPS 199 security categorization of the information residing on the media, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used.

(2) The organization documents, where appropriate, activities associated with the transport of information system media using [*Assignment: organization-defined system of records*].

Enhancement Supplemental Guidance: Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk.

(3) The organization employs an identified custodian at all times to transport information system media.

Enhancement Supplemental Guidance: Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk.

LOW Not Selected	**MOD** MP-5 (1) (2)	**HIGH** MP-5 (1) (2) (3)

MP-6 MEDIA SANITIZATION AND DISPOSAL

Control: The organization sanitizes information system media, both digital and non-digital, prior to disposal or release for reuse.

Supplemental Guidance: Sanitization is the process used to remove information from information system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or disposed. The organization uses its discretion on sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposed. NIST Special Publication 800-88 provides guidance on media sanitization. The National Security Agency also provides media sanitization guidance and maintains a listing of approved sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

Control Enhancements:

(1) The organization tracks, documents, and verifies media sanitization and disposal actions.

(2) The organization periodically tests sanitization equipment and procedures to verify correct performance.

LOW MP-6	**MOD** MP-6	**HIGH** MP-6 (1) (2)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

Supplemental Guidance: The physical and environmental protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW PE-1	**MOD** PE-1	**HIGH** PE-1

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control: The organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials. Designated officials within the organization review and approve the access list and authorization credentials [*Assignment: organization-defined frequency, at least annually*].

Supplemental Guidance: Appropriate authorization credentials include, for example, badges, identification cards, and smart cards. The organization promptly removes from the access list personnel no longer requiring access to the facility where the information system resides.

Control Enhancements: None.

LOW PE-2	**MOD** PE-2	**HIGH** PE-2

PE-3 PHYSICAL ACCESS CONTROL

Control: The organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Supplemental Guidance: The organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems. The organization secures keys, combinations, and other access devices and inventories those devices regularly. The organization changes combinations and keys: (i) periodically; and (ii) when keys are lost, combinations are compromised, or individuals are transferred or terminated. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being appropriately controlled. Where ~~federal~~Federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST Special Publication 800-73. If the token-based access control function employs cryptographic verification, the access control system conforms to the requirements of NIST Special Publication 800-78. If the token-based access control function employs biometric verification, the access control system conforms to the requirements of NIST Special Publication 800-76.

Control Enhancements:

(1) The organization controls physical access to the information system independent of the physical access controls for the facility.

Enhancement Supplemental Guidance: This control enhancement, in general, applies to server rooms, communications centers, or any other areas within a facility containing large concentrations of information system components or components with a higher impact level than that of the majority of the facility. The intent is to provide an additional layer of physical security for those areas where the organization may be more vulnerable due to the concentration of information system components or the impact level of the components. The control enhancement is not intended to apply to workstations or peripheral devices that are typically dispersed throughout the facility and used routinely by organizational personnel.

LOW PE-3	**MOD** PE-3	**HIGH** PE-3 (1)

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities.

Supplemental Guidance: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** PE-4

PE-5 ACCESS CONTROL FOR DISPLAY MEDIUM

Control: The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.

Supplemental Guidance: None.

Control Enhancements: None.

LOW Not Selected	MOD PE-5	HIGH PE-5

PE-6 MONITORING PHYSICAL ACCESS

Control: The organization monitors physical access to the information system to detect and respond to physical security incidents.

Supplemental Guidance: The organization reviews physical access logs periodically and investigates apparent security violations or suspicious physical access activities. Response to detected physical security incidents is part of the organization's incident response capability.

Control Enhancements:

(1) The organization monitors real-time physical intrusion alarms and surveillance equipment.

(2) The organization employs automated mechanisms to recognize potential intrusions and initiate appropriate response actions.

LOW PE-6	MOD PE-6 (1)	HIGH PE-6 (1) (2)

PE-7 VISITOR CONTROL

Control: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than in areas designated as publicly accessible.

Supplemental Guidance: Government contractors and others with permanent authorization credentials are not considered visitors. Personal Identity Verification (PIV) credentials for ~~federal~~Federal employees and contractors conform to FIPS 201, and the issuing organizations for the PIV credentials are accredited in accordance with the provisions of NIST Special Publication 800-79.

Control Enhancements:

(1) The organization escorts visitors and monitors visitor activity, when required.

LOW PE-7	MOD PE-7 (1)	HIGH PE-7 (1)

PE-8 ACCESS RECORDS

Control: The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the visitor access records [*Assignment: organization-defined frequency*].

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the maintenance and review of access records.

(2) The organization maintains a record of all physical access, both visitor and authorized individuals.

LOW PE-8	**MOD** PE-8	**HIGH** PE-8 (1) (2)

PE-9 POWER EQUIPMENT AND POWER CABLING

Control: The organization protects power equipment and power cabling for the information system from damage and destruction.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs redundant and parallel power cabling paths.

LOW Not Selected	**MOD** PE-9	**HIGH** PE-9

PE-10 EMERGENCY SHUTOFF

Control: The organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.

Supplemental Guidance: Facilities containing concentrations of information system resources may include, for example, data centers, server rooms, and mainframe rooms.

Control Enhancements:

(1) The organization protects the emergency power-off capability from accidental or unauthorized activation.

LOW Not Selected	**MOD** PE-10	**HIGH** PE-10 (1)

PE-11 EMERGENCY POWER

Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

(2) The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.

LOW Not Selected	**MOD** PE-11	**HIGH** PE-11 (1)

PE-12 EMERGENCY LIGHTING

Control: The organization employs and maintains automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.

Supplemental Guidance: None.

Control Enhancements: None.

LOW PE-12	**MOD** PE-12	**HIGH** PE-12

PE-13 FIRE PROTECTION

Control: The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.

Supplemental Guidance: Fire suppression and detection devices/systems include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Control Enhancements:

(1) The organization employs fire detection devices/systems that activate automatically and notify the organization and emergency responders in the event of a fire.

(2) The organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders.

(3) The organization employs an automatic fire suppression capability in facilities that are not staffed on a continuous basis.

LOW PE-13	**MOD** PE-13 (1) (2) (3)	**HIGH** PE-13 (1) (2) (3)

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control: The organization regularly maintains, within acceptable levels, and monitors the temperature and humidity within the facility where the information system resides.

Supplemental Guidance: None.

Control Enhancements: None.

LOW PE-14	**MOD** PE-14	**HIGH** PE-14

PE-15 WATER DAMAGE PROTECTION

Control: The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a significant water leak.

LOW PE-15	**MOD** PE-15	**HIGH** PE-15 (1)

PE-16 DELIVERY AND REMOVAL

Control: The organization authorizes and controls information system-related items entering and exiting the facility and maintains appropriate records of those items.

Supplemental Guidance: The organization controls delivery areas and, if possible, isolates the areas from the information system and media libraries to avoid unauthorized physical access.

Control Enhancements: None.

LOW PE-16	**MOD** PE-16	**HIGH** PE-16

PE-17 ALTERNATE WORK SITE

Control: The organization employs appropriate management, operational, and technical information system security controls at alternate work sites.

Supplemental Guidance: The organization provides a means for employees to communicate with information system security staff in case of security problems. NIST Special Publication 800-46 provides guidance on security in telecommuting and broadband communications.

Control Enhancements: None.

LOW Not Selected	**MOD** PE-17	**HIGH** PE-17

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

Control: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards.

Control Enhancements:

(1) The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

LOW Not Selected	**MOD** PE-18	**HIGH** PE-18 (1)

PE-19 INFORMATION LEAKAGE

Control: The organization protects the information system from information leakage due to electromagnetic signal~~s~~ emanations.

Supplemental Guidance: The FIPS 199 security categorization (for confidentiality) of the information system and organizational security policy guides the application of safeguards and countermeasures employed to protect the information system against information leakage due to electromagnetic signals emanations.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: PLANNING **CLASS:** MANAGEMENT

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

Supplemental Guidance: The security planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-18 provides guidance on security planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW PL-1	**MOD** PL-1	**HIGH** PL-1

PL-2 SYSTEM SECURITY PLAN

Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.

Supplemental Guidance: The security plan is aligned with the organization's information system architecture and information security architecture. NIST Special Publication 800-18 provides guidance on security planning.

Control Enhancements: None.

LOW PL-2	**MOD** PL-2	**HIGH** PL-2

PL-3 SYSTEM SECURITY PLAN UPDATE

Control: The organization reviews the security plan for the information system [*Assignment: organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.

Supplemental Guidance: Significant changes are defined in advance by the organization and identified in the configuration management process. NIST Special Publication 800-18 provides guidance on security plan updates.

Control Enhancements: None.

LOW PL-3	**MOD** PL-3	**HIGH** PL-3

PL-4 RULES OF BEHAVIOR

Control: The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

Supplemental Guidance: Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy. NIST Special Publication 800-18 provides guidance on preparing rules of behavior.

Control Enhancements: None.

LOW PL-4	**MOD** PL-4	**HIGH** PL-4

PL-5 PRIVACY IMPACT ASSESSMENT

Control: The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.

Supplemental Guidance: OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002.

Control Enhancements: None.

LOW PL-5	**MOD** PL-5	**HIGH** PL-5

PL-6 SECURITY-RELATED ACTIVITY PLANNING

Control: The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

Supplemental Guidance: Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations.

Control Enhancements: None.

LOW Not Selected	**MOD** PL-6	**HIGH** PL-6

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

Supplemental Guidance: The personnel security policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW PS-1	**MOD** PS-1	**HIGH** PS-1

PS-2 POSITION CATEGORIZATION

Control: The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations [*Assignment: organization-defined frequency*].

Supplemental Guidance: Position risk designations are consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance.

Control Enhancements: None.

LOW PS-2	**MOD** PS-2	**HIGH** PS-2

PS-3 PERSONNEL SCREENING

Control: The organization screens individuals requiring access to organizational information and information systems before authorizing access.

Supplemental Guidance: Screening is consistent with: (i) 5 CFR 731.106; (ii) Office of Personnel Management policy, regulations, and guidance; (iii) organizational policy, regulations, and guidance; (iv) FIPS 201 and Special Publications 800-73, 800-76, and 800-78; and (v) the criteria established for the risk designation of the assigned position.

Control Enhancements: None.

LOW PS-3	**MOD** PS-3	**HIGH** PS-3

PS-4 PERSONNEL TERMINATION

Control: The organization, upon termination of individual employment, terminates information system access, conducts exit interviews, retrieves all organizational information system-related property, and provides appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems.

Supplemental Guidance: Information system-related property includes, for example, keys, identification cards, and building passes. Timely execution of this control is particularly essential for employees or contractors terminated for cause.

Control Enhancements: None.

LOW PS-4	**MOD** PS-4	**HIGH** PS-4

PS-5 PERSONNEL TRANSFER

Control: The organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions.

Supplemental Guidance: Appropriate actions that may be required include: (i) returning old and issuing new keys, identification cards, building passes; (ii) closing old accounts and establishing new accounts; (iii) changing system access authorizations; and (iv) providing for access to official records created or controlled by the employee at the old work location and in the old accounts.

Control Enhancements: None.

LOW PS-5	**MOD** PS-5	**HIGH** PS-5

PS-6 ACCESS AGREEMENTS

Control: The organization completes appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements [*Assignment: organization-defined frequency*].

Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.

Control Enhancements: None.

LOW PS-6	**MOD** PS-6	**HIGH** PS-6

PS-7 THIRD-PARTY PERSONNEL SECURITY

Control: The organization establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance.

Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents. NIST Special Publication 800-35 provides guidance on information technology security services.

Control Enhancements: None.

LOW PS-7	**MOD** PS-7	**HIGH** PS-7

PS-8 PERSONNEL SANCTIONS

Control: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Supplemental Guidance: The sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The sanctions process can be included as part of the general personnel policies and procedures for the organization.

Control Enhancements: None.

LOW PS-8	**MOD** PS-8	**HIGH** PS-8

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

Supplemental Guidance: The risk assessment policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-30 provides guidance on the assessment of risk. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW RA-1	**MOD** RA-1	**HIGH** RA-1

RA-2 SECURITY CATEGORIZATION

Control: The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.

Supplemental Guidance: The applicable ~~federal~~Federal standard for security categorization of nonnational security information and information systems is FIPS 199. The organization conducts FIPS 199 security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, information system owners, and information owners. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and restricting or prohibiting network access in accordance with an organizational assessment of risk. NIST Special Publication 800-60 provides guidance on determining the security categories of the information types resident on the information system. Related security controls: MP-4, SC-7.

Control Enhancements: None.

LOW RA-2	**MOD** RA-2	**HIGH** RA-2

RA-3 RISK ASSESSMENT

Control: The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).

Supplemental Guidance: Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing ~~federal~~Federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to ~~federal~~Federal information systems. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to ~~federal~~Federal information systems. NIST Special Publication 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments.

Control Enhancements: None.

LOW RA-3	**MOD** RA-3	**HIGH** RA-3

RA-4 RISK ASSESSMENT UPDATE

Control: The organization updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.

Supplemental Guidance: The organization develops and documents specific criteria for what is considered significant change to the information system. NIST Special Publication 800-30 provides guidance on conducting risk assessment updates.

Control Enhancements: None.

LOW RA-4	**MOD** RA-4	**HIGH** RA-4

RA-5 VULNERABILITY SCANNING

Control: The organization scans for vulnerabilities in the information system [*Assignment: organization-defined frequency*] or when significant new vulnerabilities potentially affecting the system are identified and reported.

Supplemental Guidance: Vulnerability scanning is conducted using appropriate scanning tools and techniques. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code). NIST Special Publication 800-42 provides guidance on network security testing. NIST Special Publication 800-40 (Version 2) provides guidance on patch and vulnerability management.

Control Enhancements:

(1) The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.

(2) The organization updates the list of information system vulnerabilities scanned [*Assignment: organization-defined frequency*] or when significant new vulnerabilities are identified and reported.

(3) The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of scan coverage, including vulnerabilities checked and information system components scanned.

LOW Not Selected	**MOD** RA-5	**HIGH** RA-5 (1) (2)

FAMILY: SYSTEM AND SERVICES DEVELOPMENT[A1] MANAGEMENT & ACQUISITION **CLASS:**

SA-1 SYSTEM AND SERVICES DEVELOPMENT & ACQUISITION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services development & acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services development & acquisition policy and associated system and services development & acquisition controls.

Supplemental Guidance: The system and services development & acquisition policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and services development & acquisition policy can be included as part of the general information security policy for the organization. System and services development & acquisition procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW SA-1	**MOD** SA-1	**HIGH** SA-1

SA-2 ALLOCATION OF RESOURCES

Control: The organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system.

Supplemental Guidance: The organization includes the determination of security requirements for the information system in mission/business case planning and establishes a discrete line item for information system security in the organization’s programming and budgeting documentation. NIST Special Publication 800-65 provides guidance on integrating security into the capital planning and investment control process.

Control Enhancements: None.

LOW SA-2	**MOD** SA-2	**HIGH** SA-2

SA-3 LIFE CYCLE SUPPORT

Control: The organization manages the information system using a system development life cycle methodology that includes information security considerations.

Supplemental Guidance: NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle.

Control Enhancements: None.

LOW SA-3	**MOD** SA-3	**HIGH** SA-3

SA-4 ACQUISITIONS

Control: The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.

Supplemental Guidance:

Solicitation Documents
The solicitation documents (e.g., Requests for Proposals) for information systems and services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. NIST Special Publication 800-36 provides guidance on the selection of information security products. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle.

Information System Documentation
The solicitation documents include requirements for appropriate information system documentation. The documentation addresses user and systems administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the FIPS 199 security category for the information system.

Use of Tested, Evaluated, and Validated Products
NIST Special Publication 800-23 provides guidance on the acquisition and use of tested/evaluated information technology products.

Configuration Settings and Implementation Guidance
The information system required documentation includes security configuration settings and security implementation guidance. OMB FISMA reporting instructions provide guidance on configuration requirements for ~~federal~~Federal information systems. NIST Special Publication 800-70 provides guidance on configuration settings for information technology products.

Control Enhancements:

(1) The organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

(2) The organization requires in solicitation documents that appropriate documentation be provided 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).

LOW SA-4	**MOD** SA-4 (1)	**HIGH** SA-4 (1)

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.

Supplemental Guidance: Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.

Control Enhancements:

(1) The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

(2) The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, 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).

LOW SA-5	**MOD** SA-5 (1)	**HIGH** SA-5 (1) (2)

SA-6 SOFTWARE USAGE RESTRICTIONS

Control: The organization complies with software usage restrictions.

Supplemental Guidance: Software and associated documentation are used in accordance with contract agreements and copyright laws. For software and associated documentation protected by quantity licenses, the organization employs tracking systems to control copying and distribution. The organization controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Control Enhancements: None.

LOW SA-6	**MOD** SA-6	**HIGH** SA-6

SA-7 USER INSTALLED SOFTWARE

Control: The organization enforces explicit rules governing the installation of software by users.

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software that is free only for personal, not government use, and software whose pedigree with regard to being potentially malicious is unknown or suspect).

Control Enhancements: None.

LOW SA-7	**MOD** SA-7	**HIGH** SA-7

SA-8 SECURITY ENGINEERING PRINCIPLES

Control: The organization designs and implements the information system using security engineering principles.

Supplemental Guidance: NIST Special Publication 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.

Control Enhancements: None.

LOW Not Selected	**MOD** SA-8	**HIGH** SA-8

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

Control: The organization: (i) requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements; and (ii) monitors security control compliance.

Supplemental Guidance: An external information system service is a service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. Ultimately, the responsibility for adequately mitigating risks to the organization's operations and assets, and to individuals, arising from the use of external information system services remains with the authorizing official. Authorizing officials must require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information system security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk to its operations and assets, or to individuals. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-64 provides guidance on the security considerations in the system development life cycle.

Control Enhancements: None.

LOW SA-9	**MOD** SA-9	**HIGH** SA-9

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Control: The organization requires that information system developers create and implement 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.

Supplemental Guidance: This control also applies to the development actions associated with information system changes.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** SA-10

SA-11 DEVELOPER SECURITY TESTING

Control: The organization requires that information system developers create a security test and evaluation plan, implement the plan, and document the results.

Supplemental Guidance: Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security certification and accreditation process for the delivered information system. Related security controls: CA-2, CA-4.

Control Enhancements: None.

LOW Not Selected	**MOD** SA-11	**HIGH** SA-11

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

Supplemental Guidance: The system and communications protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW SC-1	**MOD** SC-1	**HIGH** SC-1

SC-2 APPLICATION PARTITIONING

Control: The information system separates user functionality (including user interface services) from information system management functionality.

Supplemental Guidance: The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-2	**HIGH** SC-2

SC-3 SECURITY FUNCTION ISOLATION

Control: The information system isolates security functions from nonsecurity functions.

Supplemental Guidance: The information system isolates security functions from nonsecurity functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.

Control Enhancements:

(1) The information system employs underlying hardware separation mechanisms to facilitate security function isolation.

(2) The information system isolates critical security functions (i.e., functions enforcing access and information flow control) from both nonsecurity functions and from other security functions.

(3) The information system minimizes the number of nonsecurity functions included within the isolation boundary containing security functions.

(4) The information system security functions are implemented as largely independent modules that avoid unnecessary interactions between modules.

(5) The information system security functions are implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

LOW Not Selected	**MOD** Not Selected	**HIGH** SC-3

SC-4 INFORMATION REMNANCE

Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance: Control of information system remnance, sometimes referred to as object reuse, or data remnance, prevents information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-4	**HIGH** SC-4

SC-5 DENIAL OF SERVICE PROTECTION

Control: The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list*].

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy.

Control Enhancements:

(1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.

(2) The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

LOW SC-5	**MOD** SC-5	**HIGH** SC-5

SC-6 RESOURCE PRIORITY

Control: The information system limits the use of resources by priority.

Supplemental Guidance: Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-7 BOUNDARY PROTECTION

Control: The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Supplemental Guidance: Any connections to the Internet, or other external networks or information systems, occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an organizational assessment of risk. FIPS 199 security categorization guides the selection of appropriate candidates for domain partitioning.

The organization carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST Special Publication 800-77 provides guidance on virtual private networks. Related security controls: MP-4, RA-2.

Control Enhancements:

(1) The organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces.

Enhancement Supplemental Guidance: Publicly accessible information system components include, for example, public web servers.

(2) The organization prevents public access into the organization's internal networks except as appropriately mediated.

(3) The organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.

(4) The organization implements a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.

(5) The information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).

(6) The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.

LOW SC-7	**MOD** SC-7 (1) (2) (3) (4) (5)	**HIGH** SC-7 (1) (2) (3) (4) (5) (6)

SC-8 TRANSMISSION INTEGRITY

Control: The information system protects the integrity of transmitted information.

Supplemental Guidance: If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST Special Publication 800-52 provides guidance on protecting transmission integrity using Transport Layer Security (TLS). NIST Special Publication 800-77 provides guidance on protecting transmission integrity using IPsec. NIST Special Publication 800-81 provides guidance on Domain Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.

Control Enhancements:

(1) **The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.**

Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems.

LOW Not Selected	**MOD** SC-8	**HIGH** SC-8 (1)

SC-9 TRANSMISSION CONFIDENTIALITY

Control: The information system protects the confidentiality of transmitted information.

Supplemental Guidance: If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST Special Publication 800-52 provides guidance on protecting transmission confidentiality using Transport Layer Security (TLS). NIST Special Publication 800-77 provides guidance on protecting transmission confidentiality using IPsec. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems. Related security control: AC-17.

Control Enhancements:

(1) **The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.**

Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems.

LOW Not Selected	**MOD** SC-9	**HIGH** SC-9 (1)

SC-10 NETWORK DISCONNECT

Control: The information system terminates a network connection at the end of a session or after [*Assignment: organization-defined time period*] of inactivity.

Supplemental Guidance: The organization applies this control within the context of risk management that considers specific mission or operational requirements.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-10	**HIGH** SC-10

SC-11 TRUSTED PATH

Control: The information system establishes a trusted communications path between the user and the following security functions of the system: [*Assignment: organization-defined security functions to include at a minimum, information system authentication and reauthentication*].

Supplemental Guidance: A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-12	**HIGH** SC-12

SC-13 USE OF CRYPTOGRAPHY

Control: For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Supplemental Guidance: The applicable ~~federal~~Federal standard for employing cryptography in nonnational security information systems is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. NIST Special Publications 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.

Control Enhancements: None.

LOW SC-13	**MOD** SC-13	**HIGH** SC-13

SC-14 PUBLIC ACCESS PROTECTIONS

Control: The information system protects the integrity and availability of publicly available information and applications.

Supplemental Guidance: None.

Control Enhancements: None.

LOW SC-14	**MOD** SC-14	**HIGH** SC-14

SC-15 COLLABORATIVE COMPUTING

Control: The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.

Supplemental Guidance: Collaborative computing mechanisms include, for example, video and audio conferencing capabilities. Explicit indication of use includes, for example, signals to local users when cameras and/or microphones are activated.

Control Enhancements:

(1) The information system provides physical disconnect of camera and microphone in a manner that supports ease of use.

LOW Not Selected	**MOD** SC-15	**HIGH** SC-15

SC-16 TRANSMISSION OF SECURITY PARAMETERS

Control: The information system reliably associates security parameters with information exchanged between information systems.

Supplemental Guidance: Security parameters include, for example, security labels and markings. Security parameters may be explicitly or implicitly associated with the information contained within the information system.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control: The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

Supplemental Guidance: For user certificates, each agency either establishes an agency certification authority cross-certified with the Federal Bridge Certification Authority at medium assurance or higher or uses certificates from an approved, shared service provider, as required by OMB Memorandum 05-24. NIST Special Publication 800-32 provides guidance on public key technology. NIST Special Publication 800-63 provides guidance on remote electronic authentication.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-17	**HIGH** SC-17

SC-18 MOBILE CODE

Control: The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of mobile code within the information system.

Supplemental Guidance: Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the information system. NIST Special Publication 800-28 provides guidance on active content and mobile code.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-18	**HIGH** SC-18

SC-19 VOICE OVER INTERNET PROTOCOL

Control: The organization: (i) establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of VoIP within the information system.

Supplemental Guidance: NIST Special Publication 800-58 provides guidance on security considerations for VoIP technologies employed in information systems.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-19	**HIGH** SC-19

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Control: The information system that provides name/address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.

Supplemental Guidance: This control enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data. NIST Special Publication 800-81 provides guidance on secure domain name system deployment.

Control Enhancements:

(1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.

Enhancement Supplemental Guidance: An example means to indicate the security status of child subspaces is through the use of delegation signer resource records.

LOW Not Selected	**MOD** SC-20	**HIGH** SC-20

SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Control: The information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.

Supplemental Guidance: A resolving or caching domain name system (DNS) server is an example of an information system that provides name/address resolution service for local clients and authoritative DNS servers are examples of authoritative sources. NIST Special Publication 800-81 provides guidance on secure domain name system deployment.

Control Enhancements:

(1) The information system performs data origin authentication and data integrity verification on all resolution responses whether or not local clients explicitly request this service.

Enhancement Supplemental Guidance: Local clients include, for example, DNS stub resolvers.

LOW Not Selected	**MOD** Not Selected	**HIGH** SC-21

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

Control: The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.

Supplemental Guidance: A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). If organizational information technology resources are divided into those resources belonging to internal networks and those resources belonging to external networks, authoritative DNS servers with two roles (internal and external) are established. The DNS server with the internal role provides name/address resolution information pertaining to both internal and external information technology resources while the DNS server with the external role only provides name/address resolution information pertaining to external information technology resources. The list of clients who can access the authoritative DNS server of a particular role is also specified. NIST Special Publication 800-81 provides guidance on secure DNS deployment.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-22	**HIGH** SC-22

SC-23 SESSION AUTHENTICITY

Control: The information system provides mechanisms to protect the authenticity of communications sessions.

Supplemental Guidance: This control focuses on communications protection at the session, versus packet, level. The intent of this control is to implement session-level protection where needed (e.g., in service-oriented architectures providing web-based services). NIST Special Publication 800-52 provides guidance on the use of transport layer security (TLS) mechanisms. NIST Special Publication 800-77 provides guidance on the deployment of IPsec virtual private networks (VPNs) and other methods of protecting communications sessions. NIST Special Publication 800-95 provides guidance on secure web services.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-23	**HIGH** SC-23

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

Supplemental Guidance: The system and information integrity policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW SI-1	**MOD** SI-1	**HIGH** SI-1

SI-2 FLAW REMEDIATION

Control: The organization identifies, reports, and corrects information system flaws.

Supplemental Guidance: The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling are also addressed expeditiously. Flaw remediation is incorporated into configuration management as an emergency change. NIST Special Publication 800-40, provides guidance on security patch installation and patch management. Related security controls: CA-2, CA-4, CA-7, CM-3, IR-4, SI-11.

Control Enhancements:

(1) The organization centrally manages the flaw remediation process and installs updates automatically.

(2) The organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.

LOW SI-2	**MOD** SI-2 (2)	**HIGH** SI-2 (1) (2)

SI-3 MALICIOUS CODE PROTECTION

Control: The information system implements malicious code protection.

Supplemental Guidance: The organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) transported: (i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., USB devices, diskettes or compact disks), or other common means; or (ii) by exploiting information system vulnerabilities. The organization updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. The organization considers using malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). The organization also considers the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. NIST Special Publication 800-83 provides guidance on implementing malicious code protection.

Control Enhancements:

(1) The organization centrally manages malicious code protection mechanisms.

(2) The information system automatically updates malicious code protection mechanisms.

LOW SI-3	**MOD** SI-3 (1) (2)	**HIGH** SI-3 (1) (2)

SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES

Control: The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.

Supplemental Guidance: Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Monitoring devices are strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices are also deployed at ad hoc locations within the system to track specific transactions. Additionally, these devices are used to track the impact of security changes to the information system. The granularity of the information collected is determined by the organization based upon its monitoring objectives and the capability of the information system to support such activities. Organizations consult appropriate legal counsel with regard to all information system monitoring activities. Organizations heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. NIST Special Publication 800-61 provides guidance on detecting attacks through various types of security technologies. NIST Special Publication 800-83 provides guidance on detecting malware-based attacks through malicious code protection software. NIST Special Publication 800-92 provides guidance on monitoring and analyzing computer security event logs. NIST Special Publication 800-94 provides guidance on intrusion detection and prevention. Related security control: AC-8.

Control Enhancements:

(1) The organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.

(2) The organization employs automated tools to support near-real-time analysis of events.

(3) The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

(4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.

Enhancement Supplemental Guidance: Unusual/unauthorized activities or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to an external information system.

(5) The information system provides a real-time alert when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined list of compromise indicators*].

LOW Not Selected	**MOD** SI-4 (4)	**HIGH** SI-4 (2) (4) (5)

SI-5 SECURITY ALERTS AND ADVISORIES

Control: The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.

Supplemental Guidance: The organization documents the types of actions to be taken in response to security alerts/advisories. The organization also maintains contact with special interest groups (e.g., information security forums) that: (i) facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies); (ii) provide access to advice from security professionals; and (iii) improve knowledge of security best practices. NIST Special Publication 800-40 provides guidance on monitoring and distributing security alerts and advisories.

Control Enhancements:

(1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

LOW SI-5	**MOD** SI-5	**HIGH** SI-5 (1)

SI-6 SECURITY FUNCTIONALITY VERIFICATION

Control: The information system verifies the correct operation of security functions [*Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every* [*Assignment: organization-defined time-period*]] and [*Selection (one or more): notifies system administrator, shuts the system down, restarts the system*] when anomalies are discovered.

Supplemental Guidance: The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required.

Control Enhancements:

(1) The organization employs automated mechanisms to provide notification of failed automated security tests.

(2) The organization employs automated mechanisms to support management of distributed security testing.

LOW Not Selected	**MOD** Not Selected	**HIGH** SI-6

SI-7 SOFTWARE AND INFORMATION INTEGRITY

Control: The information system detects and protects against unauthorized changes to software and information.

Supplemental Guidance: The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.

Control Enhancements:

(1) The organization reassesses the integrity of software and information by performing [*Assignment: organization-defined frequency*] integrity scans of the system.

(2) The organization employs automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification.

(3) The organization employs centrally managed integrity verification tools.

LOW Not Selected	**MOD** Not Selected	**HIGH** SI-7 (1) (2)

SI-8 SPAM PROTECTION

Control: The information system implements spam protection.

Supplemental Guidance: The organization employs spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet accesses, or other common means. Consideration is given to using spam protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). NIST Special Publication 800-45 provides guidance on electronic mail security.

Control Enhancements:

(1) The organization centrally manages spam protection mechanisms.

(2) The information system automatically updates spam protection mechanisms.

LOW Not Selected	**MOD** SI-8	**HIGH** SI-8 (1)

SI-9 INFORMATION INPUT RESTRICTIONS

Control: The organization restricts the capability to input information to the information system to authorized personnel.

Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

Control Enhancements: None.

LOW Not Selected	**MOD** SI-9	**HIGH** SI-9

SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY

Control: The information system checks information for accuracy, completeness, validity, and authenticity.

Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.

Control Enhancements: None.

LOW Not Selected	**MOD** SI-10	**HIGH** SI-10

SI-11 ERROR HANDLING

Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.

Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Control Enhancements: None.

LOW Not Selected	**MOD** SI-11	**HIGH** SI-11

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION

Control: The organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Supplemental Guidance: None.

Control Enhancements: None.

LOW Not Selected	**MOD** SI-12	**HIGH** SI-12

APPENDIX G

SECURITY CONTROL MAPPINGS

RELATIONSHIP OF SECURITY CONTROLS TO OTHER U.S. NATIONAL STANDARDS AND CONTROL SETS

The mapping tables in this appendix provide organizations with a *general* indication of Special Publication 800-53 security control coverage with respect to other frequently referenced national security control standards and control sets.[49] The security control mappings are not exhaustive and are based on a broad interpretation and general understanding of the control sets being compared. The mappings are created by using the primary security topic identified in each of the Special Publication 800-53 security controls and associated control enhancements (if any) and searching for a similar security topic in the other referenced security control standards and control sets. Security controls with similar functional meaning are included in the mapping table. For example, *«requires a new example, since 27001 no longer in this appendix»*, but not exactly the same, functionality. In some instances, similar topics are addressed in the security control sets but provide a different context, perspective, or scope. *«requires a new example, since 27001 no longer in this appendix»*. And finally, the following cautionary notes are in order:

- The granularity of the security control sets being compared is not always the same. This difference in granularity makes the security control mappings less precise in some instances. Therefore, the mappings provided should be considered as a basis on which to extend the applicability and correspondance between this document and the referenced sources by creating something with greater granularity, rather than simplisticly using them as a "checklist" for the express purpose of comparing security capabilities or security implementations across information systems assessed against different control sets.
- Some of the control sets referenced in this appendix (e.g., Department of Defense Instruction 8500.2) are organized into groups of security controls with each group reflecting different levels of protection. When the security control groups reflect a hierarchical enhancement of another group, only the paragraph reference from the lowest hierarchical group where the security topic first occurred is listed in the mapping column.

Organizations are encouraged to use the mapping table only as a starting point for conducting further analyses and interpretation of control similarity and associated coverage when comparing disparate control sets.

[49] The security control mapping tables include references to: (i) NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*; (ii) GAO, *Federal Information System Controls Audit Manual*; (iii) Department of Defense Instruction 8500.2, *Information Assurance Implementation*; and (iv) Director of Central Intelligence Directive 6/3 Policy and Manual, *Protecting Sensitive Compartmented Information within Information Systems*. Within these tables the designations in the respective columns indicate the paragraph identifier(s) or number(s) in the above documents where the security controls, control objectives, or associated implementation guidance may be found.

800-53 CNTL NO.	CONTROL NAME	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[50]
Access Control					

AC-1	Access Control Policy and Procedures	15.
		16.
			---	ECAN-1
				ECPA-1
				PRAS-1
				DCAR-1
					2.B.4.e(5)
					4.B.1.a(1)(b)

AC-2	Account Management	6.1.8 15.1.1 15.1.4 15.1.5 15.1.8 15.2.2 16.1.3 16.1.5 16.2.12	AC-2.1 AC-2.2 AC-3.2 SP-4.1	IAAC-1	4.B.2.a(3)
AC-3	Access Enforcement	10.1.2 15.1.1 16.1.1 16.1.2 16.1.3 16.1.7 16.1.9 16.2.1 16.2.7 16.2.10 16.2.11 16.2.15	AC-2 AC-3.2	DCFA-1 ECAN-1 EBRU-1 PRNK-1 ECCD-1 ECSD-2	Discretionary Access Control (DAC): 4.B.2.a(2) Mandatory Access Control (MAC): 4.B.4.a(3)
AC-4	Information Flow Enforcement	---	---	EBBD-1 EBBD-2	4.B.3.a(3) 7.B.3.g
AC-5	Separation of Duties	6.1.1 6.1.2 6.1.3 15.2.1 16.1.2 17.1.5	AC-3.2 SD-1.2	ECLP-1	2.A.1 4.B.3.a(18)
AC-6	Least Privilege	16.1.2 16.1.3 17.1.5	AC-3.2	ECLP-1	4.B.2.a(10)
AC-7	Unsuccessful Login Attempts	15.1.14	AC-3.2	ECLO-1	4.B.2.a(17)(c)-(d)
AC-8	System Use Notification	16.2.13 16.3.1 17.1.9	AC-3.2	ECWM-1	4.B.1.a(6)
AC-9	Previous Logon Notification	---	AC-3.2	ECLO-2	---
AC-10	Concurrent Session Control	---	---	ECLO-1	4.B.2.a(17)(a)

[50] References in this column are to both DCI Directive 6/3 and to its Manual (Administrative update, December 2003). Paragraphs cited from the Directive are preceded by "DCID" and where there are also references for the same control from the Manual, these are preceded by "Manual." Where only paragraph numbers appear, they are references to the Manual. References to paragraphs in the Manual should be construed to encompass all subparagraphs related to those paragraphs. It should also be noted that Special Publication 800-53 contains a set of security controls that cover personnel, physical, and technical security measures, and therefore, the scope of the publication is broader than DCID 6/3. Some of the controls in Special Publication 800-53 are explicitly not included in DCID 6/3 because they are addressed in other DCID and Intelligence Community (IC) policy documents. The difference in scope/breadth between Special Publication 800-53 and DCID 6/3 impacts the degree of correlation between the two documents. Thus, the lack of a "mapping" for a particular Special Publication 800-53 control to a DCID 6/3 requirement does not mean that there is no similar IC requirement. The IC Translation Review Board provided information for the DCID 6/3 mapping.

800-53 CNTL NO.	CONTROL NAME	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[50]
AC-11	Session Lock	16.1.4	AC-3.2	PESL-1	4.B.1.a(5)
AC-12	Session Termination	16.1.4 16.2.6	AC-3.2	---	4.B.2.a(17)(b)
AC-13	Supervision and Review—Access Control	7.1.10 11.2.2 16.1.10 16.2.5 17.1.6 17.1.7	AC-4 AC-4.3 SS-2.2	ECAT-1 ECAT-2 E3.3.9	2.B.7.c 4.B.3.a(8)(b)
AC-14	Permitted Actions without Identification or Authentication	16.2.12	---	---	7.D.3.a
AC-15	Automated Marking	8.2.4 16.1.6	AC-3.2	ECML-1	4.B.2.a(11)

AC-16	Automated Labeling	16.1.6	AC-3.2	ECML-1	4.B.1.a(3)
					4.B.4.a(15)
					4.B.4.a(16)

AC-17	Remote Access	16.2.4
		16.2.8
			AC-3.2	EBRP-1
				EBRU-1
					4.B.1.a(1)(b)
					4.B.3.a(11)
					7.D.2.e

AC-18	Wireless Access Restrictions	---	---	ECCT-1
				ECWN-1
					4.B.1.a(8)
					5.B.3.a(11)

AC-19	Access Control for Portable and Mobile Devices	7.3.1 7.3.2	---	ECWN-1	8.B.6.c 9.G.4
AC-20	Use of External Information Systems	10.2.13	---	---	8.B.6.c
Awareness and Training					

AT-1	Security Awareness and Training Policy and Procedures	13.	---	PRTN-1
				DCAR-1
					DCID: B.3.c
					Manual:
					2.B.2.b(8);
					2.B.4.e(6)

AT-2	Security Awareness	13.1.4 13.1.5	---	PRTN-1	8.B.1
AT-3	Security Training	13.1 13.1.3 13.1.5	---	PRTN-1	8.B.1
AT-4	Security Training Records	13.1.2	---	---	8.B.1
AT-5	Contacts with Security Groups and Associations	---	---	---	---
Audit and Accountability					

AU-1	Audit and Accountability Policy and Procedures	17.	---	ECAT-1
				ECTB-1
				DCAR-1
					DCID: B.2.d
					Manual:
					2.B.4.e(5);
					4.B.2.a(4)

AU-2	Auditable Events	17.1.1 17.1.2 17.1.4	---	ECAR-3	4.B.2.a(4)(d)

AU-3	Content of Audit Records	17.1.1	---	ECAR-1
				ECAR-2
				ECAR-3
				ECLC-1
					4.B.2.a(4)(a)
					4.B.2.a(5)(a)

AU-4	Audit Storage Capacity	---	---	---	5.B.2.a(5)(a)(1)

800-53 CNTL NO.	CONTROL NAME	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[50]
AU-5	Response to Audit Processing Failures	---	---	---	4.B.4.a(9)(d)
AU-6	Audit Monitoring, Analysis, and Reporting	16.2.5 17.1.7 17.1.8	AC-4.3	ECAT-1 E3.3.9	4.B.4.a(10)
AU-7	Audit Reduction and Report Generation	17.1.2 17.1.7	---	ECRG-1	4.B.3.a(6)
AU-8	Time Stamps	---	---	ECAR-1	4.B.2.a(4)(a)
AU-9	Protection of Audit Information	17.1.3 17.1.4	---	ECTP-1	4.B.2.a(4)(b)
AU-10	Non-repudiation	15.1.2 17.1.1	---	DCNR-1	5.B.3.a(8)
AU-11	Audit Record Retention	17.1.4	---	ECRR-1	4.B.2.a(4)(c)
Certification, Accreditation, and Security Assessments					
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	2. 4.	---	DCAR-1 DCII-1	DCID: B.3 Manual: 2.B.2.b(1)

CA-2	Security Assessments	2.1.1
		2.1.3
		2.1.4
			SP-5.1	DCII-1
				ECMT-1
				PEPS-1
				E3.3.10
					DCID: B.2.b;
					B.3.a
					Manual:
					4.B.2.b(6);
					5.B.1.b(1);
					9.B.1;
					9.B.4

CA-3	Information System Connections	1.1.1 3.2.9 4.1.8 12.2.3	CC-2.1	DCID-1 EBCR-1 EBRU-1 EBPW-1 ECIC-1	9.B.3 9.D.3.c

CA-4	Security Certification	2.1.2
		3.2.3
		3.2.5
		3.2.6
		4.1.1
		4.1.6
		11.2.8
		12.2.5
			CC-2.1	DCAR-1
				5.7.5
					DCID: B.3
					Manual:
					4.B.3.b(8);
					9.E.2.a(2);
					9.E.2.a(3)

CA-5	Plan of Action and Milestones	1.1.5 1.2.3 2.2.1 4.2.1	SP-5.1 SP-5.2	5.7.5	9.E.2.a(3)(a)
CA-6	Security Accreditation	3.2.7 12.2.5	---	5.7.5	DCID: B.3 Manual: 9.D.3; 9.D.4

CA-7	Continuous Monitoring	10.2.1	---	DCCB-1
				DCPR-1
				E3.3.9
					DCID: B.2.d;
					Manual:
					2.B.4.e(7);
					2.B.5.c(10);
					5.B.2.b(2);
					9.B.1;
					9.D.7

Configuration Management					

800-53 CNTL NO.	CONTROL NAME	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[50]

CM-1	Configuration Management Policy and Procedures	---	---	DCCB-1
				DCPR-1
				DCAR-1
				E3.3.8
					DCID: B.2.a
					Manual:
					2.B.4.e(5);
					5.B.2.a(5)

CM-2	Baseline Configuration	1.1.1
		3.1.9
		10.2.7
		10.2.9
		12.1.4
			CC-2.3
			CC-3.1
			SS-1.2
				DCHW-1
				DCSW-1
					2.B.7.c(7)
					4.B.1.c(3)
					4.B.2.b(6)

CM-3	Configuration Change Control	3.1.4
		10.2.2
		10.2.3
		10.2.8
		10.2.10
		10.2.11
			SS-3.2
			CC-2.2
				DCPR-1	2.B.7.c(7)
					4.B.1.c(3)
					4.B.2.b(6)
					5.B.2.a(5)

CM-4	Monitoring Configuration Changes	10.2.1
		10.2.4
			SS-3.1
			SS-3.2
			CC-2.1
				DCPR-1
				E3.3.8
					2.B.7.c(7)
					4.B.1.c(3)
					5.B.2.b(2)
					8.B.8.c(7)

CM-5	Access Restrictions for Change	6.1.3 6.1.4 10.1.1 10.1.4 10.1.5	SD-1.1 SS-1.2 SS-2.1	DCPR-1 ECSD-2	5.B.3.a(2)(b)
CM-6	Configuration Settings	10.2.6 10.3.1 16.2.2 16.2.3 16.2.11	---	DCSS-1 ECSC-1 E3.3.8	4.B.2.a(10)
CM-7	Least Functionality	10.3.1	---	DCPP-1 ECIM-1 ECVI-1 E3.3.8	4.B.2.a(10) 7.D.2.b

CM-8	Information System Component Inventory	1.1.1
		3.1.9
		10.2.7
		10.2.9
		12.1.4
			CC-2.3
			CC-3.1
			SS-1.2
				DCHW-1
				DCSW-1
					2.B.7.c(7)
					4.B.1.c(3)
					4.B.2.b(6)

Contingency Planning					

CP-1	Contingency Planning Policy and Procedures	9.	---	COBR-1
				DCAR-1
					2.B.4.e(5)
					6.B.1.a(1)

CP-2	Contingency Plan	4.1.4 9.1.1 9.2 9.2.1 9.2.2 9.2.3 9.2.10 12.1.8 12.2.2	SC-3.1 SC-1.1	CODP-1 COEF-1	6.B.2.b(1)
CP-3	Contingency Training	9.3.2	SC-2.3	PRTN-1	8.B.1
CP-4	Contingency Plan Testing and Exercises	4.1.4 9.3.3	SC-3.1	COED-1	6.B.3.b(2)(b)
CP-5	Contingency Plan Update	9.3.1 9.3.3 10.2.12	SC-2.1 SC-3.1	DCAR-1	6.B.3.b(2)

800-53 CNTL NO.	CONTROL NAME	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[50]

CP-6	Alternate Storage Site	9.2.4
		9.2.5
		9.2.7
		9.2.9
			SC-2.1
			SC-3.1
				CODB-2	6.B.2.a(2)
					6.B.3.a(2)(d)

CP-7	Alternate Processing Site	9.1.3 9.2.4 9.2.5 9.2.7 9.2.9	SC-2.1 SC-3.1	COAS-1 COEB-1 COSP-1 COSP-2	6.B.3.a(2)(d)
CP-8	Telecommunications Services	---	---	---	6.B.2.a(4)
CP-9	Information System Backup	9.1.1 9.2.6 9.2.9 9.3.1 12.1.9	SC-2.1	CODB-1 CODB-2 COSW-1	6.B.1.a(2)

CP-10	Information System Recovery and Reconstitution	9.2.8	SC-2.1	COTR-1
				ECND-1
					4.B.1.a(4)
					6.B.1.a(1)
					6.B.2.a(3)(d)

Identification and Authentication					
IA-1	Identification and Authentication Policy and Procedures	11.2.3	---	IAIA-1 DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5)
IA-2	User Identification and Authentication	15.1	---	IAIA-1	4.B.2.a(7)
IA-3	Device Identification and Authentication	16.2.7	---	---	4.B.5.a(14)
IA-4	Identifier Management	15.1.1 15.2.2 15.1.8	AC-2.1 AC-3.2 SP-4.1	IAGA-1 IAIA-1	4.B.1.a(2)

IA-5	Authenticator Management	15.1.6
		15.1.7
		15.1.9
		15.1.10
		15.1.11
		15.1.12
		15.1.13
		16.1.3
		16.2.3
			AC-3.2	IAKM-1
				IATS-1
					4.B.2.a(7)
					4.B.3.a(11)

IA-6	Authenticator Feedback	---	---	---	4.B.2.a(7)(g)
IA-7	Cryptographic Module Authentication	16.1.7	---	---	1.G
Incident Response					

IR-1	Incident Response Policy and Procedures	14.	---	VIIR-1
				DCAR-1
					DCID: B.2.c; C.4
					Manual:
					2.B.4.e(5);
					2.B.2.b(6);
					2.B.6.c(10);
					8.B.7

IR-2	Incident Response Training	14.1.4	SP-3.4	VIIR-1	8.B.1.b(1)(f)
					8.B.1.c(1)(e)
					8.B.1.c(2)(c)

IR-3	Incident Response Testing and Exercises	---	---	VIIR-1	8.B.7

800-53 CNTL NO.	CONTROL NAME	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[50]
IR-4	Incident Handling	2.1.5 14.1.1 14.1.2 14.1.6	SP-3.4	VIIR-1 E3.3.9	8.B.7 9.B.2.e
IR-5	Incident Monitoring	14.1.3	---	VIIR-1	8.B.7.a
IR-6	Incident Reporting	14.1.2 14.1.3 14.2.1 14.2.2 14.2.3	---	VIIR-1 E3.3.9	8.B.7
IR-7	Incident Response Assistance	8.1.1 14.1.1	SP-3.4	---	8.B.7.c
Maintenance					
MA-1	System Maintenance Policy and Procedures	10.	---	PRMP-1 DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5); 6.B.2.a(5)
MA-2	Controlled Maintenance	10.1.1 10.1.3 10.2.1	SS-3.1	---	6.B.2.a(5) 8.B.8.c

MA-3	Maintenance Tools	10.1.3
		11.2.4
			---	---	6.B.3.a(5)
					8.B.8.c(4)
					8.B.8.c(5)

MA-4	Remote Maintenance	10.1.1 17.1.1	SS-3.1	EBRP-1	8.B.8.d
MA-5	Maintenance Personnel	10.1.1 10.1.3	SS-3.1	PRMP-1	8.B.8.a
MA-6	Timely Maintenance	9.1.2	SC-1.2	COMS-1 COSP-1	6.B.2.a(5)
Media Protection					
MP-1	Media Protection Policy and Procedures	8.2	---	PESP-1 DCAR-1	DCID: B.2.a Manual: 2.B.6.c(7); 8.B.2

MP-2	Media Access	8.2.1
		8.2.2
		8.2.3
		8.2.6
		8.2.7
			---	PEDI-1
				PEPF-1
					2.B.9.b(4)
					4.B.1.a(1)
					4.B.1.a(7)

MP-3	Media Labeling	8.2.5 8.2.6 10.2.9	---	ECML-1	2.B.9.b(4) 8.B.2.a 8.B.2.c

MP-4	Media Storage	7.1.4
		8.2.1
		8.2.2
		8.2.9
		10.1.2
			AC-3.1	PESS-1	2.B.9.b(4)
					4.B.1.a(7)

MP-5	Media Transport	8.2.2 8.2.4	---	---	2.B.9.b(4)
MP-6	Media Sanitization and Disposal	3.2.11 3.2.12 3.2.13 8.2.8 8.2.9 8.2.10	AC-3.4	PECS-1 PEDD-1	8.B.5 2.B.9.b(4) 8.B.5.a(4) 8.B.5.d 8.B.5.e

800-53 CNTL NO.	CONTROL NAME	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[50]
Physical and Environmental Protection					
PE-1	Physical and Environmental Protection Policy and Procedures	7.		PETN-1 DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5); 8.D
PE-2	Physical Access Authorizations	7.1.1 7.1.2	AC-3.1	PECF-1	4.B.1.a(1) 8.E
PE-3	Physical Access Control	7.1.1 7.1.2 7.1.5 7.1.6 7.1.8	AC-3.1	PEPF-1	4.B.1.a(1) 8.D.2 8.E
PE-4	Access Control for Transmission Medium	7.2.2 16.2.9	---	---	8.D.2 4.B.1.a(8)
PE-5	Access Control for Display Medium	7.2.1	---	PEDI-1 PEPF-1	8.C.2.a 8.D.2
PE-6	Monitoring Physical Access	7.1.9	AC-4	PEPF-2	4.B.1.a(1) 8.C.2.a 8.D.2
PE-7	Visitor Control	7.1.7 7.1.11	AC-3.1	PEVC-1	8.C.2.a 8.D.2 8.E
PE-8	Access Records	7.1.9	AC-4	PEPF-2 PEVC-1	8.C.2.a 8.D.2 8.E
PE-9	Power Equipment and Power Cabling	7.1.16	SC-2.2	---	8.D.2
PE-10	Emergency Shutoff	---	---	PEMS-1	8.D.2

PE-11	Emergency Power	7.1.18	SC-2.2	COPS-1
				COPS-2
				COPS-3
					6.B.2.a(6)
					6.B.2.a(7)

PE-12	Emergency Lighting	---	---	PEEL-1	8.D.2
PE-13	Fire Protection	7.1.12	SC-2.2	PEFD-1 PEFS-1	8.C.2.a 8.D.2
PE-14	Temperature and Humidity Controls	7.1.14 7.1.15	SC-2.2	PEHC-1 PETC-1	8.D.2
PE-15	Water Damage Protection	7.1.17	SC-2.2	---	8.C.2.a 8.D.2
PE-16	Delivery and Removal	7.1.3	AC-3.1	---	8.B.5.e
PE-17	Alternate Work Site	---	---	EBRU-1	---
PE-18	Location of Information System Components	---	---	---	---
PE-19	Information Leakage	---	---	---	---
Planning					
PL-1	Security Planning Policy and Procedures	5.	---	DCAR-1 E3.4.6	DCID: B.2.a Manual: 2.B.4.e(5)

800-53 CNTL NO.	CONTROL NAME	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[50]

PL-2	System Security Plan	4.1.5
		5.1.1
		5.1.2
		12.2.1
			SP-2.1	DCSD-1	1.F.6
					2.B.6.c(3)
					2.B.7.c(5)
					9.E.2.a(1)(d)
					9.F.2.a
					Appendix C

PL-3	System Security Plan Update	3.2.10 5.2.1	SP-2.1	5.7.5	2.B.7.c(5)
PL-4	Rules of Behavior	4.1.3 13.1.1	---	PRRB-1	2.B.9.b
PL-5	Privacy Impact Assessment	---	---	---	DCID: B.3.a Manual: 8.B.9
PL-6	Security-Related Activity Planning	---	---	---	---
Personnel Security					
PS-1	Personnel Security Policy and Procedures	6.	---	PRRB-1 DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5); 8.E
PS-2	Position Categorization	6.1.1 6.1.2	SD-1.2	---	8.E

PS-3	Personnel Screening	6.2.1
		6.2.3
			SP-4.1	PRAS-1	2.B.7.c(2)
					2.B.8.b(5)
					8.E

PS-4	Personnel Termination	6.1.7	SP-4.1	5.12.7	2.B.9.b(6)
					4.B.2.a(3)(e)
					8.E

PS-5	Personnel Transfer	6.1.7	SP-4.1	5.12.7	2.B.9.b(6)
PS-6	Access Agreements	6.1.5 6.2.2	SP-4.1	PRRB-1	1.E.2 8.E
PS-7	Third-Party Personnel Security	---	SP-4.1	5.7.10	1.A.1 8.D 8.E
PS-8	Personnel Sanctions	6.1.5	---	PRRB-1	4.B.2.a(3)(e) 8.E
Risk Assessment					
RA-1	Risk Assessment Policy and Procedures	1.	---	DCAR-1	DCID: B.3.a Manual: 2.B.4.e(5)

RA-2	Security Categorization	1.1.3
		3.1.1
			SP-1
			AC-1.1
			AC-1.2
				E3.4.2	3.C
					3.D
					9.E.2.a(1)(a)
					9.E.2.a(1)(d)

800-53 CNTL NO.	CONTROL NAME	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[50]
RA-3	Risk Assessment	1.1.2 1.1.4 1.1.5 1.1.6 1.2.1 1.2.2 1.2.3 3.1.7 3.1.8 4.1.7 7.1.13 7.1.19 12.2.4	SP-1	DCDS-1 DCII-1 E3.3.10	9.B
RA-4	Risk Assessment Update	1.1.2 4.1.2	SP-1	DCAR-1 DCII-1	9.B.4.f 9.D.1.d

RA-5	Vulnerability Scanning	10.3.2
		14.2.1
			---	ECMT-1
				VIVM-1
					4.B.3.a(8)(b)
					4.B.3.b(6)(b)
					9.B.4.e

System and Services Acquisition					
SA-1	System and Services Acquisition Policy and Procedures	3.	---	DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5)
SA-2	Allocation of Resources	3.1.2 3.1.3 3.1.5 5.1.3	---	DCPB-1 E3.3.4	DCID: C.2.a Manual: 2.B.4.e(8)
SA-3	Life Cycle Support	3.1	---	5.8.1	DCID: B.2.a Manual: 9.E.2
SA-4	Acquisitions	3.1.6 3.1.7 3.1.10 3.1.11 3.1.12	---	DCAS-1 DCDS-1 DCIT-1 DCMC-1	DCID: B.2.a; C.2.a Manual: 9.B.4

SA-5	Information System Documentation	3.2.3
		3.2.4
		3.2.8
		12.1.1
		12.1.2
		12.1.3
		12.1.6
		12.1.7
			CC-2.1	DCCS-1
				DCHW-1
				DCID-1
				DCSD-1
				DCSW-1
				ECND-1
				DCFA-1
					4.B.2.b(2)
					4.B.2.b(3)
					4.B.4.b(4)
					9.C.3

SA-6	Software Usage Restrictions	10.2.10 10.2.13	SS-3.2 SP-2.1	DCPD-1	2.B.9.b(11)
SA-7	User Installed Software	10.2.10	SS-3.2	---	2.B.9.b(11)
SA-8	Security Engineering Principles	3.2.1	---	DCBP-1 DCCS-1 E3.4.4	1.H.1
SA-9	External Information System Services	12.2.3	---	DCDS-1 DCID-1 DCIT-1 DCPP-1	1.B.1 8.C.2 8.E
SA-10	Developer Configuration Management	---	SS-3.1 CC-3	---	4.B.4.b(4) 8.C.2.a

800-53 CNTL NO.	CONTROL NAME	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[50]
SA-11	Developer Security Testing	3.2.1 3.2.2 10.2.5 12.1.5	SS-3.1 CC-2.1	E3.4.4	4.B.4.b(4)
System and Communications Protection					
SC-1	System and Communications Protection Policy and Procedures	---	---	DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5)

SC-2	Application Partitioning	---	---	DCPA-1	4.B.3.b(6)(a)
					4.B.4.b(8)
					5.B.3.b(2)

SC-3	Security Function Isolation	---	---	DCSP-1	4.B.3.b(6)(a)
					4.B.4.b(8)
					5.B.3.b(1)
					5.B.3.b(2)

SC-4	Information Remnance	---	AC-3.4	ECRC-1	4.B.2.a(14)
SC-5	Denial of Service Protection	---	---	---	6.B.3.a(6)
SC-6	Resource Priority	---	---	---	6.B.3.a(11)
SC-7	Boundary Protection	16.2.2 16.2.7 16.2.9 16.2.10 16.2.11 16.2.14	AC-3.2	COEB-1 EBBD-1 ECIM-1 ECVI-1	4.B.4.a(27) 5.B.3.a(11)(b) 7.A.3 7.B 7.C 7.D
SC-8	Transmission Integrity	11.2.1 11.2.4 11.2.9 16.2.14	AC-3.2	ECTM-1	5.B.3.a(11)
SC-9	Transmission Confidentiality	---	---	ECCT-1	4.B.1.a(8)(a)
SC-10	Network Disconnect	16.2.6	AC-3.2	---	4.B.2.a(17)
SC-11	Trusted Path	16.2.7	---	---	4.B.4.a(14)
SC-12	Cryptographic Key Establishment and Management	16.1.7 16.1.8	---	IAKM-1	1.G
SC-13	Use of Cryptography	16.1.7 16.1.8	---	IAKM-1 IATS-1	1.G.1
SC-14	Public Access Protections	---	---	EBPW-1	---
SC-15	Collaborative Computing	---	---	ECVI-1	7.G
SC-16	Transmission of Security Parameters	16.1.6	AC-3.2	ECTM-2	4.B.1.a(3)

SC-17	Public Key Infrastructure Certificates	---	---	IAKM-1	2.B.4.e(5)
					4.B.3.a(11)

SC-18	Mobile Code	---	---	DCMC-1	2.B.4.e(5) 7.E
SC-19	Voice Over Internet Protocol	---	---	ECVI-1	---[51]
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	---	---	---	---

[51] Appropriate authorizing officials approve the use of specific technologies, including Voice Over Internet Protocol. See also DCID 6/3 paragraph 2.B.4.d and 9.D.1.a.

800-53 CNTL NO.	CONTROL NAME	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[50]
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	---	---	---	---
SC-22	Architecture and Provisioning for Name/Address Resolution Service	---	---	---	---
SC-23	Session Authenticity	---	---	---	---
System and Information Integrity					

SI-1	System and Information Integrity Policy and Procedures	11.	---	DCAR-1	DCID: B.2.a
					Manual:
					2.B.4.e(5)
					5.B.1.b(1)
					5.B.2.a(5)(a)(1)

SI-2	Flaw Remediation	10.3.2
		11.1.1
		11.1.2
		11.2.2
		11.2.7
			SS-2.2	DCSQ-1
				DCCT-1
				VIVM-1
					5.B.2.a(5)(a)(3)
					6.B.2.a(5)

SI-3	Malicious Code Protection	11.1.1
		11.1.2
			---	ECVP-1
				VIVM-1
					5.B.1.a(4)
					7.B.4.b(1)

SI-4	Information System Monitoring Tools and Techniques	11.2.5
		11.2.6
			---	EBBD-1
				EBVC-1
				ECID-1
					4.B.2.a(5)(b)
					4.B.3.a(8)(b)
					6.B.3.a(8)

SI-5	Security Alerts and Advisories	14.1.1 14.1.2 14.1.5	SP-3.4	VIVM-1	8.B.7

SI-6	Security Functionality Verification	11.2.1
		11.2.2
			SS-2.2	DCSS-1	4.B.1.c(2)
					5.B.2.b(2)

SI-7	Software and Information Integrity	11.2.1
		11.2.4
			---	ECSD-2	4.B.1.c(2)
					5.B.1.a(3)
					5.B.2.a(6)

SI-8	Spam Protection	---	---	---	5.B.1.a(4)
SI-9	Information Input Restrictions	---	SD-1	---	2.B.9.b(11)
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	---	---	---	7.B.2.h 2.B.4.d
SI-11	Error Handling	---	---	---	2.B.4.d
SI-12	Information Output Handling and Retention	---	---	PESP-1	2.B.4.d 8.B.9 8.G

APPENDIX H

STANDARDS AND GUIDANCE MAPPINGS

CROSSWALK BETWEEN NIST STANDARDS AND GUIDELINES AND SECURITY CONTROLS

The mapping table in this appendix provides organizations with a two-way crosswalk between NIST security standards and guidance documents (i.e., the current version of the FIPS Publications and Special Publications in the 800- series) and the security controls in the catalog of controls listed in Appendix F. The first crosswalk maps a specific NIST security publication to the associated security controls in NIST Special Publication 800-53 that are relevant to that publication. The second crosswalk maps each security control in Special Publication 800-53 to the appropriate NIST standards and guidance documents that apply to that particular control.[52] The purpose of the crosswalk is to provide organizations with additional useful information regarding security control selection and implementation. The two-way crosswalk between publications and security controls and security controls and publications is not intended to be exhaustive. In addition to providing useful information for organizations, the crosswalk also indicates particular areas where additional security guidance might be needed.

[52] There are certain FIPS and NIST Special Publications that are listed in the crosswalk for a particular security control in Appendix H that do not appear in the supplemental guidance for that control. The supplemental guidance for security controls lists only the most relevant NIST publications associated with that control or the publications that provide the most extensive guidance for that security control area.

CROSSWALK ONE: NIST PUBLICATIONS TO SECURITY CONTROLS

PUBLICATION NO.	PUBLICATION TITLE	RELATED SECURITY CONTROLS
FIPS 140-2	Security Requirements for Cryptographic Modules, May 2001	IA-7, SC-12, SC-13
FIPS 180-2	Secure Hash Standard (SHS), August 2002	SC-13
FIPS 186-2	Digital Signature Standard (DSS), January 2000	SC-13
FIPS 188	Standard Security Labels for Information Transfer, September 1994	AC-16
FIPS 190	Guideline for the Use of Advanced Authentication Technology Alternatives, September 1994	IA-1, IA-5, SC-13
FIPS 197	Advanced Encryption Standard, November 2001	SC-13
FIPS 198	The Keyed-Hash Message Authentication Code (HMAC), March 2002	AU-10, SC-8, SC-13
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems, February 2004	PL-2, RA-2
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems, March 2006	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PS-1, RA-1, SA-1, SC-1, SI-1
FIPS 201-1	Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006	AC-1, AC-3, AC-17, IA-1, IA-2, IA-4, IA-5, PL-5, SC-13, SC-17
SP 800-12	An Introduction to Computer Security: The NIST Handbook, October 1995	AC-1, AC-2, AC-3, AC-6, AC-13, AC-16, AT-1, AU-1, AU-2, AU-3, AU-6, AU-7, AU-9, CA-1, CM-1, CP-1, CP-2, CP-4, IA-1, IA-2, IR-1, MA-1, MP-1, PE-1, PE-3, PE-4, PE-13, PL-1, PL-2, PL-5, PS-1, PS-2, PS-3, PS-4, PS-5, RA-1, RA-3, RA-4, SA-1, SA-3, SC-1, SC-12, SC-13, SC-14, SI-1
SP 800-13	Telecommunications Security Guidelines for Telecommunications Management Network, October 1995	CP-8, RA-3, RA-4
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, CP-2, CP-5, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PS-1, PS-4, RA-1, RA-3, RA-4, SA-1, SA-3, SC-1, SI-1
SP 800-15	Minimum Interoperability Specification for PKI Components (MISPC), Version 1, September 1997	SC-17
SP 800-16	Information Technology Security Training Requirements: A Role- and Performance-Based Model, April 1998	AT-3
SP 800-17	Modes of Operation Validation System (MOVS): Requirements and Procedures, February 1998	CA-2, SC-13
SP 800-18	Guide for Developing Security Plans for Federal Information Systems, February 2006	CA-3, CA-5, PL-1, PL-2, PL-3
SP 800-19	Mobile Agent Security, October 1999	AC-1, AC-3, AC-6, AU-3, AU-9, PL-2, PL-5, RA-3, RA-4, SC-2, SI-3, SI-7

PUBLICATION NO.	PUBLICATION TITLE	RELATED SECURITY CONTROLS
SP 800-20	Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures, April 2000	CA-2, SC-13
SP 800-21-1	Second Edition, Guideline for Implementing Cryptography in the Federal Government, December 2005	CP-9, CP-10, PL-2, SA-3, SC-12, SC-13
SP 800-22	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, May 2001	CA-2, SC-13
SP 800-23	Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, August 2000	CA-1, CA-2, RA-3, RA-4, SA-4
SP 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does, August 2000	AC-17, CP-10, IA-2, MA-2, MP-6, PE-3, RA-3, RA-4, RA-5
SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication, October 2000	CP-9, IA-1, IA-5, PL-2, RA-3, RA-4, SC-17
SP 800-26	Security Self-Assessment Guide for Information Technology Systems, November 2001	CA-1, CA-2, CA-7, PL-2, RA-2
SP 800-27	Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A, June 2004	PL-2, SA-3, SA-8
SP 800-28	Guidelines on Active Content and Mobile Code, October 2001	AC-6, RA-3, RA-4, SC-1, SC-7, SC-15, SC-18, SI-2
SP 800-29	A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2, June 2001	SC-13
SP 800-30	Risk Management Guide for Information Technology Systems, July 2002	CA-5, PL-2, RA-1, RA-2, RA-3, RA-4, SA-3
SP 800-31	Intrusion Detection Systems (IDS), November 2001	IR-4, PL-2, RA-3, RA-4, RA-5, SA-4, SI-1, SI-4, SI-7
SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure, February 2001	IA-5, PL-2, RA-3, RA-4, SC-17, SC-20
SP 800-33	Underlying Technical Models for Information Technology Security, December 2001	PL-2, SA-8
SP 800-34	Contingency Planning Guide for Information Technology Systems, June 2002	CP-1, CP-2, CP-3, CP-4, CP-5, CP-6, CP-7, CP-8, CP-9, CP-10, MA-1, PL-2, RA-3, RA-4, SA-3
SP 800-35	Guide to Information Technology Security Services, October 2003	CA-2, CM-2, CM-8, SA-1, SA-2, SA-3, SA-9
SP 800-36	Guide to Selecting Information Technology Security Products, October 2003	AC-1, CA-2, IA-1, IR-4, MP-6, RA-5, SA-1, SA-4, SC-7, SC-17, SI-3, SI-4
SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004	CA-1, CA-2, CA-4, CA-5, CA-6, CA-7, CM-1, PL-2, PL-3, RA-1, RA-2, RA-3, RA-4, RA-5

PUBLICATION NO.	PUBLICATION TITLE	RELATED SECURITY CONTROLS
SP 800-38A	Recommendation for Block Cipher Modes of Operation - Methods and Techniques, December 2001	SC-13
SP 800-38B	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005	SC-13
SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, May 2004	SC-13
SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication (Draft), April 2006	SC-13
SP 800-40	Creating a Patch and Vulnerability Management Program, Version 2, November 2005	AT-3, AT-5, CM-2, CM-6, CM-8, PL-2, RA-2, RA-3, RA-4, RA-5, SI-2, SI-4, SI-5
SP 800-41	Guidelines on Firewalls and Firewall Policy, January 2002	AC-1, AC-4, CP-9, PL-2, SC-7
SP 800-42	Guideline on Network Security Testing, October 2003	AU-6, CA-7, PL-1, RA-3, RA-4, RA-5, SI-3, SI-4
SP 800-43	Systems Administration Guidance for Windows 2000 Professional, November 2002	AC-2, CM-6, SI-2, CP-9, CP-10
SP 800-44	Guidelines on Securing Public Web Servers, September 2002	AC-1, AC-17, AU-1, AU-2, AU-6, AU-7, IA-2, CM-6, CP-9, CP-10, IA-1, PL-2, PL-5, RA-3, RA-4, RA-5, SC-5, SC-7, SC-8, SC-9, SI-4, SI-7, SI-10
SP 800-45A	Guidelines on Electronic Mail Security (Draft), August 2006	AC-1, AC-17, AU-2, AU-6, AU-9, CM-6, CP-9, IA-1, PL-2. PL-4, RA-3, RA-4, RA-5, SC-8, SC-9, SI-3, SI-8
SP 800-46	Security for Telecommuting and Broadband Communications, August 2002	AC-1, AC-17, AC-18, AC-20, CM-6. IA-1, IA-2, PL-4, RA-3, RA-4, RA-5, SC-7, SC-10
SP 800-47	Security Guide for Interconnecting Information Technology Systems, August 2002	CA-3
SP 800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, November 2002	AC-18, CM-6, IA-3, PL-4, RA-3, RA-4, SI-4
SP 800-49	Federal S/MIME V3 Client Profile, November 2002	AU-10, SC-8, SC-9
SP 800-50	Building an Information Technology Security Awareness and Training Program, October 2003	AT-1, AT-2, AT-3, AT-4, CP-3, IR2
SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme, September 2002	RA-5, SI-2, SI-5
SP 800-52	Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, June 2005	AU-10, IA-3, SC-8, SC-9, SC-12, SC-23
SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems (Second Public Draft), April 2006	CA-2

PUBLICATION NO.	PUBLICATION TITLE	RELATED SECURITY CONTROLS
SP 800-54	Border Gateway Protocol Security (Draft), September 2006	CM-6, RA-3, RA-4, SC-5, SC-7, SC-8, SC-9, SC-23
SP 800-55	Security Metrics Guide for Information Technology Systems, July 2003	CA-1, CA-2, CA-4, CA-7, RA-3, RA-4
SP 800-56A	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2006	CP-4, SC-12, SC-17
SP 800-57	Recommendation on Key Management, August 2005	AC-16, AU-1, CP-9, CP-10, MP-5, PL-2, SC-8, SC-9, SC-12, SC-17, SI-7, SI-10
SP 800-58	Security Considerations for Voice Over IP Systems, January 2005	AC-4, AC-17, AC-18, IA-3, PE-4, PE-11, PL-2, SC-7, SC-8, SC-9, SC-12, SC-16, SC-19
SP 800-59	Guideline for Identifying an Information System as a National Security System, August 2003	RA-2
SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004	RA-2, RA-3, RA-4
SP 800-61	Computer Security Incident Handling Guide, January 2004	IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-7, SI-5
SP 800-63	Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology, Version 1.0.2, April 2006	IA-1, IA-5, RA-3, RA-4
SP 800-64	Security Considerations in the Information System Development Life Cycle, Revision 1, June 2004	PL-2, SA-1, SA-2, SA-3, SA-4
SP 800-65	Integrating Security into the Capital Planning and Investment Control Process, January 2005	CA-5, PL-1, RA-3, RA-4, SA-1, SA-2
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, March 2005	AC-1, AC-2, AC-3, AC-5, AC-6, AT-1, AT-2, AT-3, AU-1, AU-2, CA-1, CA-2, CA-3, CA-4, CA-6, CP-1, CP-2, CP-4, IA-4, IA-5, IR-1, MP-1, MP-4, MP-6, PE-1, PE-3, PE-18, PL-1, PS-1, PS-4, PS-8, RA-1, RA-2, RA-3, RA-4, SA-1, SA-9, SC-8, SC-9, SI-1, SI-7
SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, May 2004	SC-13
SP 800-68	Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist, October 2005	AC-3, AC-6, AC-7, AC-17, AU-2, AU-4, CM-6, IA-2, IA-5, SC-5
SP 800-69	Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist, September 2006	AC-6, CP-9, IA-2, SI-3
SP 800-70	Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers, May 2005	CM-6, SC-7
SP 800-72	Guidelines on PDA Forensics, November 2004	AU-1, AU-2, AU-9, IA-3, IA-4, IA-6, MP-1, MP-2, MP-5

PUBLICATION NO.	PUBLICATION TITLE	RELATED SECURITY CONTROLS
SP 800-73	Interfaces for Personal Identity Verification, Revision 1, April 2006	AC-3, AC-17, IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, PE-3, SC-12
SP 800-76-1	Biometric Data Specification for Personal Identity Verification (Draft), September 2006	AC-3, AC-17, CA-2, CA-4, IA-1, IA-2, IA-5, PE-3, SA-11
SP 800-77	Guide to IPsec VPNs, December 2005	AC-4, AC-17, AC-20, IA-3, IA-5, MA-4, SC-7, SC-8, SC-9, SC-12, SC-23
SP 800-78	Cryptographic Algorithms and Key Sizes for Personal Identity Verification, April 2005	AC-3, AC-17, IA-2, IA-4, IA-5, IA-7, PE-3, SC-13
SP 800-79	Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations, July 2005	CA-1, CA-2, CA-4, CA-6, CA-7
SP 800-81	Secure Domain Name System (DNS) Deployment Guide, May 2006	AC-6, CM-6, CM-7, CP-10, IA-3, PL-2, SC-3, SC-5, SC-8, SC-20, SC-21, SC-22
SP 800-82	Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security (Draft), September 2006	AC-4, CM-6, CP-2, PE-3, RA-3, RA-4, RA-5, SC-7
SP 800-83	Guide to Malware Incident Prevention and Handling, November 2005	AC-6, AU-2, AU-5, AU-6, CM-4, CM-6, CM-7, CP-10, IR-1, IR-4, RA-5, SA-7, SC-7, SI-2, SI-3, SI-4
SP 800-84	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, September 2006	CP-1, CP-3, CP-4, IR-1, IR-2, IR-3
SP 800-85A	PIV Card Application and Middleware Interface Test Guidelines, April 2006	CA-4, CA-7, SA-11, SI-6
SP 800-85B	PIV Data Model Test Guidelines, July 2006	CA-4, CA-7, SA-11, SI-6
SP 800-86	Guide to Integrating Forensic Techniques into Incident Response, August 2006	IR-1, IR-4
SP 800-87	Codes for the Identification of Federal and Federally-Assisted Organizations, January 2006	AC-3, AC-17, IA-1, IA-2, IA-4, IA-5, IA-7
SP 800-88	Guidelines for Media Sanitization, September 2006	MA-1, MP-1, MP-4, MP-6
SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications, November 2006	AU-10, PL-4, SC-17
SP 800-90	Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2006	SC-13
SP 800-92	Guide to Computer Security Log Management, September 2006	AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-11, IR-4, MP-4, MP-5, SI-4
SP 800-94	Guide to Intrusion Detection and Prevention (IDP) Systems (Draft), August 2006	AU-2, AU-3, AU-6, AU-8, AU-9, IR-4, SA-4, SC-5, SI-1, SI-3, SI-4, SI-7
SP 800-95	Guide to Secure Web Services (Draft), August 2006	AC-3, AU-10, SC-5, SC-8, SC-9, SC-23
SP 800-96	PIV Card / Reader Interoperability Guidelines, September 2006	AC-3, AC-17, IA-2, IA-3, IA-4, IA-5, PE-3
SP 800-97	Guide to IEEE 802.11i: Establishing Robust Security Networks (Draft), June 2006	AC-18, IA-2, IA-3, SC-8, SC-9, SC-12, SA-3

PUBLICATION NO.	PUBLICATION TITLE	RELATED SECURITY CONTROLS
SP 800-98	Guidance for Securing Radio Frequency Identification (RFID) Systems (Draft), September 2006	AC-3, AC-5, CP-10, MP-6, PE-3, PE-19, PL-5, RA-3, RA-4, SA-3
SP 800-100	Information Security Handbook: A Guide for Managers, October 2006	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1
SP 800-101	Guidelines on Cell Phone Forensics (Draft), August 2006	IR-4

CROSSWALK TWO: SECURITY CONTROLS TO NIST PUBLICATIONS

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
Access Control		
AC-1	Access Control Policy and Procedures	FIPS 200, 201-1; NIST Special Publications 800-12, 800-14, 800-19, 800-36, 800-41, 800-44, 800-45, 800-46, 800-66, 800-100
AC-2	Account Management	NIST Special Publications 800-12, 800-43, 800-66
AC-3	Access Enforcement	FIPS 201-1; NIST Special Publications 800-12, 800-19, 800-66, 800-68, 800-73, 800-76, 800-78, 800-87, 800-95, 800-96, 800-98
AC-4	Information Flow Enforcement	NIST Special Publications 800-41, 800-77, 800-82
AC-5	Separation of Duties	NIST Special Publication 800-66, 800-98
AC-6	Least Privilege	NIST Special Publications 800-12, 800-19, 800-28 800-66, 800-68, 800-69, 800-81, 800-83
AC-7	Unsuccessful Login Attempts	NIST Special Publication 800-68
AC-8	System Use Notification	No references available.
AC-9	Previous Logon Notification	No references available.
AC-10	Concurrent Session Control	No references available.
AC-11	Session Lock	No references available.
AC-12	Session Termination	No references available.
AC-13	Supervision and Review—Access Control	NIST Special Publication 800-12
AC-14	Permitted Actions without Identification or Authentication	No references available.
AC-15	Automated Marking	No references available.
AC-16	Automated Labeling	FIPS 188; NIST Special Publications 800-12, 800-57
AC-17	Remote Access	FIPS 201-1; NIST Special Publications 800-24, 800-44, 800-45, 800-46, 800-58, 800-68, 800-73, 800-76. 800-77, 800-78, 800-87, 800-96
AC-18	Wireless Access Restrictions	NIST Special Publications 800-46, 800-48, 800-58, 800-97
AC-19	Access Control for Portable and Mobile Systems	No references available.
AC-20	Use of External Information Systems	NIST Special Publications 800-46, 800-77
Awareness and Training		
AT-1	Security Awareness and Training Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-50, 800-66, 800-100
AT-2	Security Awareness	NIST Special Publications 800-50, 800-66
AT-3	Security Training	NIST Special Publications 800-16, 800-31, 800-40, 800-50, 800-66
AT-4	Security Training Records	NIST Special Publications 800-50
AT-5	Contacts with Security Groups and Associations	NIST Special Publications 800-40
Audit and Accountability		
AU-1	Audit and Accountability Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-44, 800-57, 800-66, 800-72, 800-92, 800-100

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
AU-2	Auditable Events	NIST Special Publications 800-12, 800-44, 800-45, 800-66, 800-68, 800-72, 800-83, 800-92, 800-94
AU-3	Content of Audit Records	NIST Special Publications 800-12, 800-19, 800-92, 800-94
AU-4	Audit Storage Capacity	NIST Special Publications 800-68, 800-92
AU-5	Response to Audit Processing Failures	NIST Special Publications 800-83, 800-92
AU-6	Audit Monitoring, Analysis, and Reporting	NIST Special Publications 800-12, 800-42, 800-44, 800-45, 800-83, 800-92, 800-94
AU-7	Audit Reduction and Report Generation	NIST Special Publications 800-12, 800-44, 800-92
AU-8	Time Stamps	NIST Special Publications 800-92, 800-94
AU-9	Protection of Audit Information	NIST Special Publications 800-12, 800-19, 800-45, 800-72, 800-92, 800-94
AU-10	Non-repudiation	FIPS 198; NIST Special Publications 800-49, 800-52, 800-89, 800-95
AU-11	Audit Record Retention	NIST Special Publication 800-92
Certification, Accreditation, and Security Assessments		
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-23, 800-26, 800-37, 800-53A, 800-66, 800-79, 800-100
CA-2	Security Assessments	NIST Special Publications 800-17, 800-20, 800-22, 800-23, 800-26, 800-35, 800-36, 800-37, 800-53A, 800-55, 800-66, 800-76, 800-79
CA-3	Information System Connections	NIST Special Publications 800-18, 800-47, 800-66
CA-4	Security Certification	NIST Special Publications 800-37, 800-53A, 800-66, 800-76, 800-79, 800-85A, 800-85B
CA-5	Plan of Action and Milestones	NIST Special Publications 800-18, 800-30, 800-37, 800-65
CA-6	Security Accreditation	NIST Special Publications 800-37, 800-66, 800-79
CA-7	Continuous Monitoring	NIST Special Publications 800-26, 800-37, 800-42, 800-53A, 800-79, 800-85A, 800-85B
Configuration Management		
CM-1	Configuration Management Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-37, 800-100
CM-2	Baseline Configuration	NIST Special Publications 800-35, 800-40, 800-82
CM-3	Configuration Change Control	No references available.
CM-4	Monitoring Configuration Changes	NIST Special Publication 800-83
CM-5	Access Restrictions for Change	No references available.
CM-6	Configuration Settings	NIST Special Publications 800-40, 800-43, 800-44, 800-45, 800-46, 800-48, 800-54, 800-68, 800-70, 800-81, 800-82, 800-83
CM-7	Least Functionality	NIST Special Publications 800-81, 800-83
CM-8	Information System Component Inventory	NIST Special Publications 800-35, 800-40
Contingency Planning		
CP-1	Contingency Planning Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-34, 800-66, 800-84, 800-100

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
CP-2	Contingency Plan	NIST Special Publications 800-12, 800-14, 800-34, 800-66
CP-3	Contingency Training	NIST Special Publications 800-34, 800-50, 800-84
CP-4	Contingency Plan Testing	NIST Special Publications 800-12, 800-34, 800-56, 800-66, 800-84
CP-5	Contingency Plan Update	NIST Special Publications 800-14, 800-34
CP-6	Alternate Storage Site	NIST Special Publication 800-34
CP-7	Alternate Processing Site	NIST Special Publication 800-34
CP-8	Telecommunications Services	NIST Special Publications 800-13, 800-34
CP-9	Information System Backup	NIST Special Publications 800-21, 800-25, 800-34, 800-41, 800-43, 800-44, 800-45, 800-57, 800-69
CP-10	Information System Recovery and Reconstitution	NIST Special Publications 800-21, 800-24, 800-34, 800-43, 800-44, 800-57, 800-81, 800-83, 800-98
	Identification and Authentication	
IA-1	Identification and Authentication Policy and Procedures	FIPS 190, FIPS 200, FIPS 201-1; NIST Special Publications 800-12, 800-14, 800-25, 800-36, 800-44, 800-45, 800-46, 800-63, 800-73, 800-76, 800-87, 800-100
IA-2	User Identification and Authentication	FIPS 201-1; NIST Special Publications 800-12, 800-24, 800-44, 800-46, 800-68, 800-69, 800-73, 800-76, 800-78, 800-87, 800-96, 800-97
IA-3	Device Identification and Authentication	NIST Special Publications 800-48, 800-52, 800-72, 800-73, 800-77, 800-81, 800-96, 800-97
IA-4	Identifier Management	FIPS 201-1; NIST Special Publications 800-66, 800-72, 800-73, 800-78, 800-87, 800-96
IA-5	Authenticator Management	FIPS 190, 201-1; NIST Special Publications 800-25, 800-32, 800-63, 800-66, 800-68, 800-73, 800-76, 800-77, 800-78, 800-87, 800-96
IA-6	Authenticator Feedback	NIST Special Publication 800-72
IA-7	Cryptographic Module Authentication	FIPS 140-2; NIST Special Publications 800-73, 800-78, 800-87
	Incident Response	
IR-1	Incident Response Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-61, 800-66, 800-86, 800-83, 800-84, 800-100
IR-2	Incident Response Training	NIST Special Publications 800-50, 800-61, 800-84
IR-3	Incident Response Testing	NIST Special Publication 800-61, 800-84
IR-4	Incident Handling	NIST Special Publications 800-31, 800-36, 800-61, 800-83, 800-86, 800-92, 800-94, 800-101
IR-5	Incident Monitoring	NIST Special Publication 800-61
IR-6	Incident Reporting	NIST Special Publication 800-61
IR-7	Incident Response Assistance	NIST Special Publication 800-61
	Maintenance	
MA-1	System Maintenance Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-34, 800-88, 800-100
MA-2	Controlled Maintenance	NIST Special Publication 800-24
MA-3	Maintenance Tools	No references available.
MA-4	Remote Maintenance	NIST Special Publication 800-77

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
MA-5	Maintenance Personnel	No references available.
MA-6	Timely Maintenance	No references available.
	Media Protection	
MP-1	Media Protection Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-66, 800-72, 800-88, 800-100
MP-2	Media Access	NIST Special Publication 800-72
MP-3	Media Labeling	No references available.
MP-4	Media Storage	NIST Special Publications 800-66, 800-88, 800-92
MP-5	Media Transport	NIST Special Publications 800-57, 800-72, 800-92
MP-6	Media Sanitization and Disposal	NIST Special Publications 800-24, 800-36, 800-66, 800-88, 800-98
	Physical and Environmental Protection	
PE-1	Physical and Environmental Protection Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-66, 800-100
PE-2	Physical Access Authorizations	No references available.
PE-3	Physical Access Control	NIST Special Publications 800-12, 800-24, 800-66, 800-73, 800-76, 800-78, 800-82, 800-96, 800-98
PE-4	Access Control for Transmission Medium	NIST Special Publications 800-12, 800-58
PE-5	Access Control for Display Medium	No references available.
PE-6	Monitoring Physical Access	No references available.
PE-7	Visitor Control	No references available.
PE-8	Access Records	No references available.
PE-9	Power Equipment and Power Cabling	No references available.
PE-10	Emergency Shutoff	No references available.
PE-11	Emergency Power	NIST Special Publication 800-58
PE-12	Emergency Lighting	No references available.
PE-13	Fire Protection	NIST Special Publication 800-12
PE-14	Temperature and Humidity Controls	No references available.
PE-15	Water Damage Protection	No references available.
PE-16	Delivery and Removal	No references available.
PE-17	Alternate Work Site	No references available.
PE-18	Location of Information System Components	NIST Special Publication 800-66
PE-19	Information Leakage	NIST Special Publication 800-98
	Planning	
PL-1	Security Planning Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-18, 800-42, 800-65, 800-66, 800-100
PL-2	System Security Plan	FIPS 199, 200; NIST Special Publications 800-12, 800-14, 800-18, 800-19, 800-21, 800-25, 800-26, 800-27, 800-30, 800-31, 800-32, 800-33, 800-34, 800-37, 800-40, 800-41, 800-44, 800-45, 800-57, 800-58, 800-64, 800-81
PL-3	System Security Plan Update	NIST Special Publications 800-18, 800-37

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
PL-4	Rules of Behavior	NIST Special Publications 800-45, 800-46, 800-48, 800-89
PL-5	Privacy Impact Assessment	FIPS 201-1; NIST Special Publications 800-12, 800-19, 800-44, 800-98
PL-6	Security-Related Activity Planning	No references available.
Personnel Security		
PS-1	Personnel Security Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-66, 800-100
PS-2	Position Categorization	NIST Special Publication 800-12
PS-3	Personnel Screening	NIST Special Publication 800-12
PS-4	Personnel Termination	NIST Special Publications 800-12, 800-14, 800-66
PS-5	Personnel Transfer	NIST Special Publication 800-12
PS-6	Access Agreements	No references available.
PS-7	Third-Party Personnel Security	No references available.
PS-8	Personnel Sanctions	NIST Special Publication 800-66
Risk Assessment		
RA-1	Risk Assessment Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-30, 800-37, 800-66, 800-100
RA-2	Security Categorization	FIPS 199; NIST Special Publications 800-26, 800-30, 800-37, 800-40, 800-59, 800-60, 800-66
RA-3	Risk Assessment	NIST Special Publications 800-12, 800-13, 800-14, 800-19, 800-23, 800-24, 800-25, 800-28, 800-30, 800-31, 800-32, 800-34, 800-37, 800-40, 800-42, 800-44, 800-45, 800-46, 800-48, 800-53A, 800-54, 800-60, 800-63, 800-65, 800-66, 800-82, 800-98
RA-4	Risk Assessment Update	NIST Special Publications 800-12, 800-13, 800-14, 800-19, 800-23, 800-24, 800-25, 800-28, 800-30, 800-31, 800-32, 800-34, 800-37, 800-40, 800-42, 800-44, 800-45, 800-46, 800-48, 800-53A, 800-54, 800-60, 800-63, 800-65, 800-66, 800-82, 800-98
RA-5	Vulnerability Scanning	NIST Special Publications 800-24, 800-31, 800-36, 800-37, 800-40, 800-42, 800-44, 800-45, 800-46, 800-51, 800-83
System and Services Acquisition		
SA-1	System and Services Acquisition Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-35, 800-36, 800-64, 800-65, 800-66, 800-100
SA-2	Allocation of Resources	NIST Special Publications 800-35, 800-64, 800-65
SA-3	Life Cycle Support	NIST Special Publications 800-12, 800-14, 800-21, 800-27, 800-30, 800-34, 800-35, 800-64, 800-97, 800-98
SA-4	Acquisitions	NIST Special Publications 800-23, 800-31, 800-36, 800-64, 800-94
SA-5	Information System Documentation	No references available.
SA-6	Software Usage Restrictions	No references available.
SA-7	User Installed Software	NIST Special Publication 800-83
SA-8	Security Engineering Principles	NIST Special Publications 800-27, 800-33
SA-9	External Information System Services	NIST Special Publications 800-35, 800-66
SA-10	Developer Configuration Management	No references available.

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
SA-11	Developer Security Testing	NIST Special Publications 800-76, 800-85A, 800-85B
System and Communications Protection		
SC-1	System and Communications Protection Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-28, 800-100
SC-2	Application Partitioning	NIST Special Publication 800-19
SC-3	Security Function Isolation	NIST Special Publication 800-81
SC-4	Information Remnance	No references available.
SC-5	Denial of Service Protection	NIST Special Publications 800-44, 800-54, 800-68, 800-81, 800-94, 800-95
SC-6	Resource Priority	No references available.
SC-7	Boundary Protection	NIST Special Publications 800-28, 800-36, 800-41, 800-44, 800-46, 800-54, 800-58, 800-70, 800-77, 800-82, 800-83
SC-8	Transmission Integrity	FIPS 198; NIST Special Publications 800-44, 800-45, 800-49, 800-52, 800-57, 800-54, 800-58, 800-66, 800-77, 800-81, 800-95, 800-97
SC-9	Transmission Confidentiality	NIST Special Publications 800-44, 800-45, 800-49, 800-52, 800-54, 800-57, 800-58, 800-66, 800-77, 800-95, 800-97
SC-10	Network Disconnect	NIST Special Publication 800-46
SC-11	Trusted Path	No references available.
SC-12	Cryptographic Key Establishment and Management	FIPS 140-2; NIST Special Publications 800-12, 800-21, 800-52, 800-56, 800-57, 800-58, 800-73, 800-77, 800-97
SC-13	Use of Cryptography	FIPS 140-2, 180-2, 186-2, 190, 197 198, 201-1; NIST Special Publications 800-12, 800-17, 800-20, 800-21, 800-22, 800-29, 800-38A, 800-38B, 800-38C, 800-38D, 800-67, 800-78, 800-90
SC-14	Public Access Protections	NIST Special Publication 800-12
SC-15	Collaborative Computing	No references available.
SC-16	Transmission of Security Parameters	No references available.
SC-17	Public Key Infrastructure Certificates	FIPS 201; NIST Special Publications 800-15, 800-25, 800-32, 800-36, 800-56, 800-57, 800-89
SC-18	Mobile Code	NIST Special Publication 800-28
SC-19	Voice Over Internet Protocol	NIST Special Publication 800-58
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	NIST Special Publications 800-32, 800-81
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	NIST Special Publication 800-81
SC-22	Architecture and Provisioning for Name/Address Resolution Service	NIST Special Publication 800-81
SC-23	Session Authenticity	NIST Special Publications 800-52, 800-54, 800-77, 800-95
System and Information Integrity		
SI-1	System and Information Integrity Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-31, 800-66, 800-94, 800-100
SI-2	Flaw Remediation	NIST Special Publications 800-28, 800-40, 800-43, 800-51, 800-83
SI-3	Malicious Code Protection	NIST Special Publications 800-19, 800-36, 800-42, 800-45, 800-69, 800-83, 800-94

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
SI-4	Information System Monitoring Tools and Techniques	NIST Special Publications 800-31, 800-36, 800-40, 800-42, 800-44, 800-48, 800-83, 800-92, 800-94
SI-5	Security Alerts and Advisories	NIST Special Publications 800-40, 800-51, 800-61
SI-6	Security Functionality Verification	NIST Special Publication 800-85A, 800-85B
SI-7	Software and Information Integrity	NIST Special Publications 800-19, 800-31, 800-44, 800-57, 800-66, 800-94
SI-8	Spam Protection	NIST Special Publication 800-45
SI-9	Information Input Restrictions	No references available.
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	NIST Special Publications 800-44, 800-57
SI-11	Error Handling	No references available.
SI-12	Information Output Handling and Retention	No references available.

APPENDIX I

INDUSTRIAL CONTROL SYSTEMS

INTERIM GUIDANCE ON THE APPLICATION OF SECURITY CONTROLS

Industrial control systems[53] are information systems that differ significantly from traditional administrative, mission support, and scientific data processing information systems. Industrial control systems have many unique characteristics—including a need for real-time response and extremely high availability, predictability, and reliability. These types of specialized systems are pervasive throughout the critical infrastructure, often being required to meet several and often conflicting safety, operational, performance, reliability, and security requirements such as: (i) minimizing risk to the health and safety of human beings; (ii) preventing serious damage to the environment; (iii) preventing serious production stoppages or slowdowns that result in negative impact to the nation's economy and ability to carry out critical functions; (iv) protecting the critical infrastructure from cyber attacks and common human error; and (v) safeguarding against the compromise of proprietary information.[54]

Until recently, industrial control systems had little resemblance to traditional information systems in that they were isolated systems running proprietary software and control protocols. However, as these systems have been increasingly integrated more closely into mainstream organizational information systems to promote connectivity, efficiency, and remote access capabilities, they have started to resemble the more traditional information systems. In many cases, industrial control systems are using the same commercially available hardware and software components as are used in the organization's traditional information systems. While the change in industrial control system architecture supports new information system capabilities, it also provides significantly less isolation for these systems from the outside world and introduces many of the same vulnerabilities that exist in current networked information systems. The result is a greater need to secure industrial control systems.

FIPS 200, in combination with NIST Special Publication 800-53, requires that ~~federal~~Federal agencies implement minimum security controls for their organizational information systems based on the FIPS 199 security categorization of those systems. This includes implementing the minimum baselines described in Special Publication 800-53 in industrial control systems that are operated by or on behalf of ~~federal~~Federal agencies. This appendix discusses the problems that agencies may encounter in applying the security controls in Special Publication 800-53 to industrial control systems and provides some observations and recommendations on how to meet the intent of the requirements until NIST develops additional guidance specific to those types of systems. The specific guidance for industrial control systems may include modifications of the current security controls and control enhancements and/or interpretations of selected security controls for the specialized environments in which the controls are applied.

[53] An industrial control system is an information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes. Industrial control systems are typically found in the electric, water, oil and gas, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (automotive, aerospace, and durable goods) industries as well as in air and rail transportation control systems.

[54] See Executive Order 13231 on Critical Infrastructure Protection, October 16, 2001.

Because today's industrial control systems are a combination of legacy systems, often with a planned life span of between twenty to thirty years, and/or are a hybrid of legacy systems augmented with today's commercially available hardware and software that are interconnected to other organizational information systems, it is often difficult or impossible to apply some of the security controls contained in Special Publication 800-53. Recognizing this problem, NIST has initiated a high-priority project in cooperation with the public and private sector industrial control system community, to develop specific guidance on the application of the security controls in Special Publication 800-53 to industrial control systems. Since the project is still ongoing, the resulting guidance could not be included in the current release of Special Publication 800-53. However, on the basis of the project results to date, NIST makes the following observations and recommendations for organizations that own and operate industrial control systems:

- Section 3.3 of Special Publication 800-53, *Tailoring the Initial Baseline*, allows the organization to modify or adjust the recommended security control baselines when certain conditions exist that require that flexibility. Based on the discussion above, NIST recommends that industrial control system owners take advantage of the ability to tailor the initial baselines when it is not possible or feasible to implement specific security controls contained in the baselines. However, all tailoring activity should, as its primary goal, focus on meeting the intent of the original security controls whenever possible or feasible. Additionally, the organization must address the residual risks present after the tailoring is completed.

- In some cases, it may be infeasible, impractical, or unsafe to implement a specific security control within an industrial control system. For example, AC-11, *Session Lock*, is required for all moderate-impact and high-impact information systems. For industrial control systems with requirements for real-time response and extremely high availability, predictability, and reliability, session lock may not make sense (e.g., locking an operator's session in an electric power distribution system or an air traffic control system). However, the purpose of the session lock control is to prevent unauthorized access to an information system when the user or operator leaves the terminal or workstation unattended for a period of time. In this case, in order to meet the intent of the session lock security control, an organization could utilize the compensating control concept described in Section 3.3. With appropriate rationale as described in the compensating control section, an organization can choose to compensate for not using session locks by incorporating other safeguards and countermeasures (e.g., increasing physical security, ensuring physical isolation of the terminal or workstation, increasing personnel security, and/or adding surveillance equipment to ensure that only authorized or trusted personnel are permitted in the vicinity of the terminal or workstation).

- Until NIST completes the industrial control system project and publishes specific guidance for industrial control systems, organizations should adjust their ongoing activities aimed at determining compliance with FIPS 200 and Special Publication 800-53 to allow for the types of flexibility that are discussed above. However, it is also reasonable to require industrial control system owners to develop a multiyear plan to demonstrate how the system owner plans to transition the industrial control system to a state that is fully compliant with FIPS 200 and Special Publication 800-53, particularly for systems that are planned to be in operation for several more years.

APPENDIX J

ISO/IEC 27001 MAPPINGS

RELATIONSHIP OF SECURITY CONTROLS TO ISO/IEC 27001

T• he mapping tables in this appendix provide organizations with a *general* indication of Special Publication 800-53 security control coverage with respect to the process and procedural requirements and reference controls in ISO/IEC 27001:2005 "Information security management systems - requirements". The security control mappings are extensive but not exhaustive and are based on a broad interpretation and general understanding of the control sets being compared. The mappings relate to the intention of the Special Publication 800-53 Security Controls and are applicable to all baselines (since the applied controls should relate in terms of their strength and application according to the risk assessment and baseline deemed to be appropriate.)

The mappings are created by using the primary security topic identified in each of the 800-53 security controls and associated control enhancements (if any) and searching for a similar security topic in the ISO/IEC 27001:2005 requirements. Procedural and process measures and security controls with similar functional purpose are included in the mapping tables. For example, Special Publication 800-53 contingency planning and ISO/IEC 27001 business continuity were deemed to have similar, but not exactly the same, scopes. In some instances, similar topics are addressed in the security control sets but provide a different context, perspective, or scope. For example, Special Publication 800-53 addresses information flow broadly in terms of assigned authorizations for controlling access between source and destination objects, whereas ISO/IEC 27001 addresses the information flow more narrowly as it applies to interconnected network domains.

It is also important to understand that Special Publication 800-53 is designed to provide assurance as to the security of information systems and as such focuses on the systems and the environment (including the information security management environment) in which the IT systems reside, and is intended to have the information system owners as its primary subjects. By contrast, ISO/IEC 27001 focuses on the information security management system (ISMS) primarily and how the management system accommodates the IT systems which fall within its scope, and therefore its primary audience is the senior management of the organizational entity which the ISMS addresses.

An important implication of this is that an ISMS is likely to be the subject of a single conformity or certification process, but the 'C&A' process within which the scope of Special Publication 800-53 sits is essentially for each single IT system, even though they may reside within a common security management framework. Thus, organizations seeking to be compliant with both assessment models need to pay regard to these subtle differences, and guidance offered in Special Publication 800-39 should be taken into account to overcome this problem.

Organizations are encouraged to use the mapping tables as a basis for determining their own specific solutions to seeking conformity with the ISO standard's requirements whilst also ensuring compliance with Special Publication 800-53 security controls, in the context of their own information system and operational and management environment.

MAPPINGS AGAINST ISO/IEC 27001:2005

The following tables map the Special Publication 800-53 security controls against the requirements of ISO/IEC 27001:2005, "*Information security management systems - Requirements*". ISO/IEC 27001 describes normative requirements for the building, operation and management of an information security management system (ISMS) in its clauses §4 to §8 inclusive and its Annex A describes a set of control objectives and controls (reference controls) which should be applied to IT systems supporting the organization's operations.

The following tables provide:

- Table J.1: A mapping from Special Publication 800-53 **processes** into the normative requirements of ISO/IEC 27001, where ISO/IEC 27001 has a matching (or similar) requirement which could reasonably be applied to meet the SP 800-53 requirement;
- Table J.2: A mapping from Special Publication 800-53 **security controls** into the normative requirements of ISO/IEC 27001, where ISO/IEC 27001 has a matching (or similar) requirement which could reasonably be applied to meet the SP 800-53 requirement;
- Table J.3: A reverse mapping which relates the ISO/IEC 27001:2005 processes, procedures and controls, and the Extended Control Set in table J.4, into the Special Publication 800-53 security processes and controls;
- Table J.4: An Extended Control Set, as a set of suggested additional security controls, expressed in the format used in ISO/IEC 27001 Annex A, which supplements the reference controls in ISO/IEC 27001 and thereby enables an organization to construct a Statement of Applicability (reference ISO/IEC 27001 §4.2.2(j)) which fully addresses the Special Publication 800-53 security controls.

Hyper-links are provided between the referencec within the tables, to facilitate cross-referencing by implementers and assessors.

Irrespective of whether the mapping is from Special Publication 800-53 to ISO/IEC 27001 or the other way, many of the mappings are one-many. This need not demand that for each original clause there be a unique solution for each of the mapped clauses in the other standard. A single process or control measure may frequently be an adequate response to the requirement to provide one or more controls in these areas. To take an example, consider the first entry in Table J.2: Control AC-1 has been mapped to no less than eighteen 27001 controls. However, many of these controls are about establishing policy and stating responsibilities (i.e. the scope of AC-1): a single policy document may be sufficient to address all policy/responsibility issues and thus satisfy many of the cited controls. It is the organization's choice to keep those policies together, as might a small organization do, or to distribute them amongst different documents which might allow delegation across the organization. That is for the organization to decide, based upon its overall policies, view of risk, its structure, etc.

In the following tables references to Special Publication 800-53 are pre-fixed with '§' where the reference is in the main body of that document, or otherwise use the control number assigned to the control in Appendix F.

References to ISO/IEC 27001 are pre-fixed with either '§' or 'A.', depending upon whether the reference is in the main body of the requirements or in Annex A, respectively.

J.1 SPECIAL PUBLICATION 800-53 ➔ ISO/IEC 27001 MAPPING (THE PROCESS)

800-53 section number	title/key text	ISO/IEC 27001 reference(s)	Comments (NB – refs to §3…. are to SP 800-53 clauses, all others are to ISO/IEC 27001 clauses/controls)
		§3.1 MANAGING RISK	
§3.1	whole section	[§4.2.2(f)]	[§3.1 refers to risk management but does not address broader operation of the ISMS, although the following mappings to §3.1.x will show that many principles are applied]
§3.1.1	Categorize	§4.2.1(b)(3,4), §4.2.1(c)	This mapping is reinforced by the assumed application of FIPS 199.
§3.1.2	Select an initial set of security controls	§4.2.1(c) §4.2.1(g)	By implication, also §4.2.1(d – f inclusive)
§3.1.3	Supplement	§4.2.1(c)), §4.2.1(d) §4.2.1(e) §4.2.1(f) §4.2.1(g)	
§3.1.4	Document	§4.2.1(j) §4.3.1(i)	Note that this step in 27001 comes after §4.2.1(h & i), but need not be sequentially to them, since knowledge of the rationale for selection may support management review and approval.
§3.1.5	Implement	§4.2.2	Since SP 800-53 is focused around controls, §4.2.2(c) is especially applicable, although all other parts of this section apply.
§3.1.6	Assess	§4.2.3, §6, §7	Subject to the caveat concerning the differing perspectives of SP 800-53 vs. 27001.
§3.1.7	Authorize	§4.2.1(h) §4.2.1(j) §4.3.1(i)	
§3.1.8	Monitor	§4.2.3 §6, §7, A.15	Control group A.15 is identified because the SP 800-53 clause requires “reporting to appropriate [] officials”, which is most likely to be a requirement of a standard or regulation
		§3.2 SECURITY CATEGORIZATION	
Whole section		§4.2.1(b)(3,4)), §4.2.1(c)	This mapping is reinforced by the assumed application of FIPS 199.
		§3.3 SELECTING AND TAILORING THE INITIAL BASELINE	
§3.3.1	***Choice of control baseline***	Title	
§3.3.1(a)	*.. scoping guidance*	§4.2.1(b)(3,4), §4.2.1(c)	
§3.3.1(b)	*... compensating security controls*	§4.2.1(g) §4.2.1(j) §4.3.1(i)	
§3.3.1(c)	*... organization-defined parameters*	§4.2.1(g) §4.2.1(h) §4.2.1(i) §4.2.1(j) §4.3.1(i)	
§3.3.2	***Scoping Guidance***	Title	
§3.3.2(a)	*Common security control-related considerations*	§4.2.1(j) §4.3.1(i)	This is a specifically-focused case of the equivalent 27001 control, implementation of which would need to make use of the Table J.2 mappings. 27001 clauses §4.2.1(d - g) are not mapped here because the use of these controls is mandatory, so no basic selection is required (although there does need to be an initial assessment of the choice of baseline).

800-53 section number	title/key text	ISO/IEC 27001 reference(s)	Comments (NB – refs to §3…. are to SP 800-53 clauses, all others are to ISO/IEC 27001 clauses/controls)
§3.3.2(b)	*Operational/environmental-related considerations*	§4.2.1(d) §4.2.1(e) §4.2.1(f) §4.2.1(g) §4.2.1(j) §4.3.1(i) A.9	The control group A.9 is generally applicable.
§3.3.2(c)	*Physical infrastructure-related considerations*	§4.2.1(d) §4.2.1(e) §4.2.1(f) §4.2.1(g) §4.2.1(j) §4.3.1(i) A.9	The control group A.9 is generally applicable.
§3.3.2(d)	*Public access-related considerations*	§4.2.1(d) §4.2.1(e) §4.2.1(f) §4.2.1(g) §4.2.1(j) A.9	Controls groups A.9, A.11 are the most applicable, but other discrete controls may also be relevant.
§3.3.2(e)	*Technology-related considerations*	§4.2.1(d) §4.2.1(e) §4.2.1(f) §4.2.1(g) §4.2.1(j) §4.3.1(i) A.9 A.10 A.11 A.12 A.15	The control group A.9 is generally applicable but with regard to the specific topics used as examples, controls in A.10, A.11, A.12 and A.15 groups are relevant.
§3.3.2(f)	*Policy-regulatory-related considerations*	§4.2.1(a) §4.2.1(b)(2), A.15.1 A.15.3	A.15.2 is explicitly excluded since it relates to standards, whereas regulation etc. may require audit as a part of governance and due diligence.
§3.3.2(g)	*Scalability-related considerations*	§4.2.1(a) §4.2.1(b)*(2, 4)*	The ISMS approach is equally able to accommodate depth and breadth in scope and complexity, and can ably accommodate the SP 800-53 process.
§3.3.2(h)	*Security objective-related considerations*	§4.2.1(b)(4)), §4.2.1(c) §4.2.1(d) §4.2.1(e) §4.2.1(f) §4.2.1(g)	Refer to mappings for controls cited in the referenced SP 800-53 process clauses.
§3.3.3	***Compensating Security Controls***	n/a	Initial paragraph is narrative.
§3.3.3(a)	*… selecting compensating controls*	§4.2.1(b)(4)), §4.2.1(c) §4.2.1(d) §4.2.1(e) §4.2.1(f) §4.2.1(g)	Mappings in Tables J.2 and J.3 support selections of compensating controls from SP 800-53; Additional controls required should supplement Table J.3 within the ISMS SoA.
§3.3.3(b)	*… rationale for compensating controls*	§4.2.1(j) §4.3.1(i)	As noted elsewhere, the strict ordering of these 27001 requirements is not essential, and the logical sequence defined in SP 800-53 is a more pragmatic approach which the ISMS schema can accommodate.
§3.3.3(c)	*… acceptance of risk related to compensating controls*	§4.2.1(h) §4.2.1(i) §4.2.1(j) §4.3.1(i)	

800-53 section number	title/key text	ISO/IEC 27001 reference(s)	Comments (NB – refs to §3…. are to SP 800-53 clauses, all others are to ISO/IEC 27001 clauses/controls)
§3.3.4	***Organization-defined Security Control Parameters***	§4.2.1(f) §4.2.1(g) §4.2.1(j) §4.3.1(a) §4.3.1(b) §4.3.1(i) A.15	Parameters within controls are not explicitly considered within 27001, but these references are the process-related points where such matters would be considered and recorded (some within the SoA, others as procedures). This clause also alludes to matters of compliance, hence the A.15 group of controls applies.
§3.4 SUPPLEMENTING THE TAILORED BASELINE			
§3.4.1	***Foundational tailored baseline***	§4.2.1(b)(3, 4), §4.2.1(c) §4.2.1(d) §4.2.1(e) §4.2.1(f) §4.2.1(g) §4.2.1(j) §4.3.1(a) §4.3.1(b) §4.3.1(i)	Essentially, this clause is a retrospective of what has gone before, hence all previous mappings from SP 800-53 §3.1 to §3.3 inclusive can be applied. The mappings to left relate to the final sentence of this clause.
§3.4.2	***Risk-based supplementation***	§4.2.1(c) §4.2.1(d) §4.2.1(e) §4.2.1(f) §4.2.1(g) §4.2.1(j) §4.3.1(a) §4.3.1(b)	Controls mapping in Tables J.2 and J.3 should be applied.
§3.4.3	***Supplementary use restrictions***	§4.2.1(c) §4.2.1(d) §4.2.1(e) §4.2.1(f) §4.2.1(g) §4.2.1(j) §4.3.1(a) §4.3.1(b) §4.3.1(i) §5, A.7, A.11.2	This clause specifically invokes management responsibility whilst also suggesting that restricting access/usage is appropriate, hence the specific controls identified.
§3.4.3(a)	*… limiting information system usage*	A.5.1, A.7, A.9, A.10, A.11	The control groups cited have specific potential for providing controls which address the clause in question
§3.4.3(b)	*… prohibiting system access*	A.11.4	The control groups cited have specific potential for providing controls which address the clause in question
§3.4.3(c)	*… prohibiting sensitive information*	A.7, A.11	The control groups cited have specific potential for providing controls which address the clause in question
§3.4.4	***Record of decisions***	§4.2.1(j) §4.3.1(i) §4.3.1(i) §7.3	Implicit within this is that §7.2 applies in that action on decisions is a necessary follow-up.
§3.5 UPDATING SECURITY CONTROLS			
§3.5.1	***Continuous monitoring of control applicability***	§4.2.2, §4.2.3, §4.2.4, §7, §8, A.12.5, A.13	Talks about event specific in next sections

800-53 section number	title/key text	ISO/IEC 27001 reference(s)	Comments (NB – refs to §3…. are to SP 800-53 clauses, all others are to ISO/IEC 27001 clauses/controls)
§3.5.2	***Event-driven review of control applicability***	A.12.5, A.13	
§3.5.2(a)	*… reconfirm criticality/sensitivity*	§4.2.3, §4.2.4, §7, §8, A.13.2.2	
§3.5,2(b)	*… (re-)assess security state and risk*	§4.2.3, §4.2.4, §7, §8, A.13	
§3.5.2(c)	*… plan and initiate corrective actions*	[A.4.2.2.(d)] §4.2.3, §4.2.4, §7, §8, A.13	[A.4.2.2(d) states "Define how to measure the effectiveness of controls"; §3.5.2(c) requires effectiveness to be measured but does not specifically require that there be established a process or framework for that.]
§3.5.2(d)	*Consider re-accrediting …*	n/a	Within 27001 itself this issue is not addressed, although if the ISMS is formally-certified a condition of certification (in accordance with ISO/IEC 27006:2007) would be to notify the certifier if any change was deemed to invalidate the validity of the certification.

J.2 SPECIAL PUBLICATION 800-53 ➔ ISO/IEC 27001 MAPPING (SECURITY CONTROLS)

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
		Access Control	
AC-1	Access Control Policy and Procedures Control:	**Primary**: §4.2.1(b) §5.1 A.5.1.1 A.5.1.2 A.6.1.3 A.8.1.1 A.9.1.1 A.9.1.2 A.9.1.3 A.11.1.1 A.11.2.1 A.11.2.2 A.11.2.3 A.11.2.4 A.11.4.1 A.11.6.1 A.11.7.1 A.11.7.2 Secondary: §4.3.1(c) A.10.1.1 A.15.1.1 A.15.2.1	A.5 is policy overall; A6 is allocation of responsibilities, A8 refers to personnel roles/responsibilities; A.9 refers to physical control (implicitly by policy, although A5 may be the anchor); A.11 is logical control, but addresses procedures, review (A.11.1.1 is just policy); A.11.4 is networks (good catch!); A.11.6 addresses restrictions determined by policy; A.11.7 addresses mobile computing and tele-working policy; A.15 addresses both regulation and standards (per AC-1 text) NOTE – As a principle, and with regard to all XX-1 controls, §4.2.1(b) is always also be considered, especially where the ISMS covers a single system, as is A.5.1.1 which is regarded as being directly applicable, since it is the primary point for policy determination: even if specific policies exist for any XX-1 domain, they should be referenced by an overall policy, which A.5.1.1 should address. As supporting 'secondary' controls, A.15.1.1, A.15.2.1 and A.15.3.1 are always considered and usually selected as being supportive of policy (because they relate to all those areas covered by the SP 800-53 'Supplemental guidance'); §4.3.1(C) and A.10.1.1 are referenced because of the overall 27001 requirement to have documented procedures. In many specific cases, ref. to A,15.3.1 may be omitted for scope reasons. It is noted that the original SP 800-53 mapping referenced only A.15.1.1 on a consistent basis.
AC-2	Account Management	**Primary**: A.6.2.2 A.6.2.3 A.8.3.3 A.11.2.1 A.11.2.2 A.11.2.3 A.11.2.4 A.11.5.1 A.11.5.2 A.11.5.5 A.11.5.6 A.11.7.2 Secondary: A.15.1.5	
AC-3	Access Enforcement	**Primary**: A.9.1.2 A.9.1.6 A.10.7.3 A.11.2.2 A.11.4.2 A.11.4.3 A.11.4.6 A.11.5.2 Secondary: A.9.2.1 A.11.6.2 A.12.4.2	

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
AC-4	Information Flow Enforcement	**Primary**: A.10.6.2 A.11.4.2 A.11.4.3 A.11.4.4 A.11.4.5 A.11.4.6 A.11.4.7 Secondary: A.11.7.2 A.12.4.2	
AC-5	Separation of Duties	**Primary**: A.10.1.3 A.10.6.1 A.11.2.1(c) Secondary: A.10.10.1	’
AC-6	Least Privilege	**Primary**: A.11.2.2(b) Secondary: A.11.1.1	A.11.1.1 is secondary, since it addresses policy, rather than strict ‘enforcement’, which the -53 control specifies (but it does say ‘the .. system’)
AC-7	Unsuccessful Login Attempts	**Primary**: A.11.5.1	
AC-8	System Use Notification	**Primary**: A.8.1.3 A.11.5.1 A.15.1.4 A.15.1.5 Secondary: A.6.2.1 A.6.2.2 A.8.1.1	External users (Joe Public) are ‘third-parties’ in ISMS-speak: thus, A.8 controls could also address the notification issue, which involves responsibility and ts&cs of use (but should not go so far as to include A.8.2.2 – awareness and training, which is much more than notification.)
AC-9	Previous Logon Notification	**Primary**: A.11.5.1	
AC-10	Concurrent Session Control	**Primary**: A.11.5.1	
AC-11	Session Lock	**Primary**: A.11.5.5	‘Lock’ and ‘Termination’ are each ‘shut down’
AC-12	Session Termination	**Primary**: A.11.5.5 Secondary: A.11.5.1	
AC-13	Supervision and Review—Access Control	**Primary**: A.9.1.2(e) A.10.2.2 A.10.6.1(de) A.10.10.1 A.10.10.2 A.10.10.4 A.13.2.1 A.15.3.1 Secondary: A.6.1.5(g) A.6.2.2(h) A.6.2.3(n) A.11.7.2 (2nd i)	
AC-14	Permitted Actions without Identification or Authentication	**Primary**: §4.2.3(d) A.11.1.1	

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
AC-15	Automated Marking	**Primary**: A.7.2.1 A.7.2.2	A.7.2.1 because of the need to determine classification and the binding of that with labeling.
AC-16	Automated Labeling	**Primary**: A.7.2.1 A.7.2.2	See above
AC-17	Remote Access	**Primary**: A.11.1.1 A.11.4.1 A.11.4.2 A.11.4.3 A.11.4.4 A.11.4.5 A.11.4.6 A.11.4.7 A.11.7.1 A.11.7.2 Secondary: A.12.3.1 A.12.3.2 A.15.1.6	
AC-18	Wireless Access Restrictions	**Primary**: A.10.6.1 (c) A.10.8.1 (e) A.11.1.1 A.11.4.2 A.11.4.5 A.11.7.1 A.11.7.2	
AC-19	Access Control for Portable and Mobile Devices	**Primary**: A.10.4.1 A.10.4.2 A.11.1.1 A.11.4.3 A.11.7.1	
AC-20	Use of External Information Systems	**Primary**: A.6.1.5 A.6.2.1 A.6.2.2 A.6.2.3 A.7.1.3 A.8.1.1 A.8.1.3 A.9.2.5 A.9.2.7 A.11.7.1	
		Awareness and Training	
AT-1	Security Awareness and Training Policy and Procedures	**Primary**: §4.2.1(b) §5.1 §5.2.2 A.8.1.1 Secondary: §4.3.1(c) A.10.1.1 A.15.1.1 A.15.2.1 A.15.3.1	

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
AT-2	Security Awareness	**Primary**: §5.2.2 A.8.2.1 A.8.2.2 Secondary: A.11.7.1	
AT-3	Security Training	**Primary**: §5.2.2 A.8.2.1 A.8.2.2 Secondary: A.11.7.1	
AT-4	Security Training Records	**Primary**: §4.3.3	
AT-5	Contacts with Security Groups and Associations	**Primary**: A.6.1.7	
	Audit and Accountability		
AU-1	Audit and Accountability Policy and Procedures	**Primary**: §4.2.1(b) §4.2.3(e) §5.1 §5.2.2 §6 A.8.1.1 A.15.3.1 Secondary: §4.3.1(c) A.10.1.1 A.15.1.1 A.15.2.1	
AU-2	Auditable Events	**Primary**: A.10.2.2 A.10.10.4 A.10.10.6 A.11.7.2(i*) A.12.4.1(f) A.12.6.1(h) A.13.2.1(c) A.15.3.1 Secondary: A.10.10.6	* In A.11.7.2 there are two sub-paragraphs bearing the reference 'h' – this refers to the second of the two.
AU-3	Content of Audit Records	**Primary**: A.10.10.1 A.10.10.4 Secondary: A.13.2.3	
AU-4	Audit Storage Capacity	**Primary**: §5.2.1(b) A.6.1.1 A.10.10.3 Secondary: A.10.3.1	Ref to A.6.1.1 is based upon guidance 27002 §6.1.1(e). Ref. A.10.10.3 is to 27002 §10.10.3(c).

AU-5	Response to Audit Processing Failures	A.10.10.3(c)
		Secondary:
		A.13.2.1(a(1) d(4))	

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
AU-6	Audit Monitoring, Analysis, and Reporting	**Primary**: §4.2.3(a) (2, 4, 5) §4.2.3(d) §6 §7.1 §7.2 §7.3 A.10.10.2 A.10.10.4 A.15.3.1 Secondary: §4.2.3(b)	Strictly the A.10.10.4 control is to 'log'; the 27002 guidance references reviewing which is consistent with the phrasing of control A.10.10.2; a note has been taken to recommend to ISO JTC1/SC27inclusion of 'and reviewed regularly' to control '.4.
AU-7	Audit Reduction and Report Generation	**Primary**: SP53.AU.1 Secondary: §4.3.3 A.10.10.3 A.15.3.2	The 27001 requirements relate to protection of audit logs, nothing to do with generating reports from them. Therefore, at best secondary relationships.
AU-8	Time Stamps	**Primary**: §4.3.3 A.10.10.6	
AU-9	Protection of Audit Information	**Primary**: §4.3.3 A.10.10.3 A.13.2.3 A.15.1.3 A.15.3.2	
AU-10	Non-repudiation	**Primary**: A.10.9.1 (d) A.11.1.1 A.11.2.1 A.11.2.2 A.11.4.1 A.11.4.2 A.11.5.1 A.11.5.2 A.12.3.1	
AU-11	Audit Record Retention	**Primary**: §4.3.1(h) §4.3.3 A.10.10.1 A.15.1.3(b) Secondary: A.13.2.3	
Certification, Accreditation, and Security Assessments			

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	**Primary**: §4.1 §4.2.1(b) §5.1 A.5.1.1 Secondary: §4.2.1 §4.2.2 §4.2.3 §4.2.4 §4.3.1(c) A.5.1.2 A.10.1.1 A.15.1.1 A.15.2.1 A.15.3.1	Essentially, this would be a basic accomplishment of undergoing **formal** certification of conformity to ISO/IEC 27001, with the certification assessment being performed by a certification body operating under the terms of ISO/IEC 27006. CA-1 addresses process for the organization which require it to have in place the steps which enable the ATO to be granted.
CA-2	Security Assessments	**Primary**: §6 A.6.1.8 Secondary: A.15.2.1 A.15.2.2	A.15.2.x are considered secondary because, although they may also be considered as equivalent to conforming to standards, were an ISMS approach to be taken to be equivalent to the FISMA requirements then this mapping would most likely be no longer required.
CA-3	Information System Connections	**Primary**: A.6.2.1 A.6.2.2 A.6.2.3 A.11.4.2 Secondary: A.6.1.4	
CA-4	Security Certification	**Primary**: §4.2.1(h) Secondary: A.5.1.1 A.10.3.2	This requirement is essentially the build-up to ATO. On the broad level, look at the ISMS §4.2 process requirements in general, in terms of their FISMA-related execution – those cited are the most directly relevant for this control; for ISMS controls, look at those cited.
CA-5	Plan of Action and Milestones	**Primary**: §4.2.1(b) §5.1 §7.1 §7.2 §7.3 A.5.1.2	
CA-6	Security Accreditation	**Primary**: §4.2.1(i) §6 Secondary: A.10.3.2	§4.2.1(i) addresses the management aspects, whereas the others can relate to the IT.
CA-7	Continuous Monitoring	**Primary**: §4.2.3 §6 §7.1 §7.2 §7.3 A.7.1.1 A.7.1.2 A.7.1.3 A.9.2.7 A.10.1.2 A.12.5.1 A.12.5.2 A.12.5.3 Secondary: §4.3.2	
Configuration Management			

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
CM-1	Configuration Management Policy and Procedures	**Primary**: §4.2.1(b) §5.1 A.5.1.1 A.5.1.2 A.12.4.1 A.12.5.1 A.12.5.3 Secondary: §4.3.1(c) A.10.1.1 A.15.1.1 A.15.2.1 A.15.3.1	
CM-2	Baseline Configuration	**Primary**: SP53.CM.1 Secondary: A.7.1.1 A.12.5.1	This is very much IT-system specific, within the overall context of good management by adoption of such practices.
CM-3	Configuration Change Control	**Primary**: A.10.1.1 A.10.1.2 A.10.2.3 A.12.4.1 A.12.5.1 A.12.5.2 A.12.5.3 Secondary: A.12.1.1	
CM-4	Monitoring Configuration Changes	**Primary**: A.12.5.2	
CM-5	Access Restrictions for Change	**Primary**: A.11.1.1 A.11.2 A.11.6.1 A.12.5.3	
CM-6	Configuration Settings	**Primary**: SP53.CM.2	
CM-7	Least Functionality	**Primary**: SP53.CM.3	
CM-8	Information System Component Inventory	**Primary**: §4.2.1(d)(1) A.7.1.1 A.7.1.2	
		Contingency Planning	
CP-1	Contingency Planning Policy and Procedures	**Primary**: §4.2.1(b) §5.1 A.5.1.1 A.5.1.2 A.14.1.1 A.14.1.2 Secondary: §4.3.1(c) A.10.1.1 A.15.1.1 A.15.1.4 A.15.2.1 A.15.3.1	

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
CP-2	Contingency Plan	**Primary**: A.14.1.2 A.14.1.3 A.14.1.4	
CP-3	Contingency Training	**Primary**: §5.2.2 A.8.2.2 A.14.1.4	
CP-4	Contingency Plan Testing and Exercises	**Primary**: A.10.5.1 A.14.1.5	
CP-5	Contingency Plan Update	**Primary**: §5.1(h) §7.1 §7.2 §7.3 A.14.1.1 (i) A.14.1.5	
CP-6	Alternate Storage Site	**Primary**: A.10.5.1 A.14.1.3 A.14.1.5 Secondary: A.6.2.1 A.6.2.2 A.6.2.3 A.14.1.4	
CP-7	Alternate Processing Site	**Primary**: A.14.1.3 A.14.1.5 Secondary: A.6.2.1 A.6.2.2 A.6.2.3 A.14.1.4	
CP-8	Telecommunications Services	**Primary**: SP53.CP.1 Secondary: A.10.2.1 A.14.1.1	
CP-9	Information System Backup	**Primary**: A.10.5.1	
CP-10	Information System Recovery and Reconstitution	**Primary**: A.14.1.3 A.14.1.4	
		Identification and Authentication	
IA-1	Identification and Authentication Policy and Procedures	**Primary**: §4.2.1(b) A.5.1.1 A.6.1.1 A.11.1.1 A.11.2.1 SP53.IA.1 Secondary: §4.3.1(c) A.10.1.1 A.15.1.1 A.15.2.1 A.15.3.1	

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
IA-2	User Identification and Authentication	**Primary**: A.11.2.1 A.11.4.2 A.11.5.2 A.11.5.3	
IA-3	Device Identification and Authentication	**Primary**: A.11.4.3 A.11.7.1	
IA-4	Identifier Management	**Primary**: A.11.2.1 Secondary: A.11.1.1	Caveat - 27001 is very, perhaps too, password-centric, rather than looking for credentials in general, although THIS control (i.e. IA-4) is itself hardware credential-centric.
IA-5	Authenticator Management	**Primary**: A.11.3.1 A.11.5.2. SP53.IA.1 Secondary: A.11.5.3	Credentials not well addressed in 27001 – A.11.5.2 is too password-centric, making only a minor reference to 'strong authentication, hence the Extended Control.
IA-6	Authenticator Feedback	**Primary**: SP53.IA.2	A.11.5.1 was considered but only very loosely relates to IA-6, being more concerned with the access to the **operating system** rather than the application itself; IA-6 is also more concerned with protection of the authentication process itself. In 27002 item (i) is the strongest linkage, and is very password-focused. Hence an additional, more focused and more widely applicable, Extended Control is justified.
IA-7	Cryptographic Module Authentication	**Primary**: A.15.1.1 A.15.1.6 A.15.2.1	
		Incident Response	
IR-1	Incident Response Policy and Procedures	**Primary**: §4.2.1(b) §5.1 A.5.1.1 A.5.1.2 A.13.1.1 Secondary: §4.3.1(c) A.10.1.1 A.15.1.1 A.15.2.1 A.15.3.1	
IR-2	Incident Response Training	**Primary**: §4.2.2(e) §5.2.2 A.8.2.2	
IR-3	Incident Response Testing and Exercises	**Primary**: SP53.IR.1 Secondary: A.14.1.5	A.14.1.5 is only a vague relationship – there is a certain separation between incident response being part of every-day operations and business continuity being related to more significant events, although there is no obvious dividing line (when does a meal become a feast?)
IR-4	Incident Handling	**Primary**: A.13.2.1	
IR-5	Incident Monitoring	**Primary**: A.13.2.2	
IR-6	Incident Reporting	**Primary**: A.6.1.6 A.13.1.1	

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
IR-7	Incident Response Assistance	**Primary**: A.13.1.2	
Maintenance			
MA-1	System Maintenance Policy and Procedures	**Primary**: §4.2.1(b) §5.1 A.5.1.1 Secondary: §4.3.1(c) A.10.1.1 A.15.1.1 A.15.2.1	
MA-2	Controlled Maintenance	**Primary**: A.9.2.4 Secondary: A.12.5.1 A.12.5.2 A.12.5.3	
MA-3	Maintenance Tools	**Primary**: A.9.2.4	
MA-4	Remote Maintenance	**Primary**: A.11.4.4	Note that whereas SP 800-53 addresses the issue from a perspective of authorization, the 27001 control comes at the issue from the opposite direction, i.e. is protection-focused. The controls therefore are the same but diametrically-opposed!
MA-5	Maintenance Personnel	**Primary**: A.12.4.3 A.12.5.1	
MA-6	Timely Maintenance	**Primary**: A.9.2.4	
Media Protection			
MP-1	Removable Media Protection Policy and Procedures	**Primary**: §4.2.1(b) §5.1 A.5.1.1 A.10.7.1 A.10.7.2 A.10.7.3 A.10.7.4 A.11.1.1 A.15.1.3 Secondary: §4.3.1(c) A.10.1.1 A.11.1.1 A.15.1.1 A.15.2.1	NB – in the context of SP 800-53 'media' are only those removable components, rather than fixed ones. A.11.1.1 is cited as part of access control in general
MP-2	Media Access	**Primary**: A.10.7.1 A.10.7.3	See comment above re 'removable'.
MP-3	Media Labeling	**Primary**: A.7.2.2 A.10.7.3 A.10.8.2(h) A.15.1.3	
MP-4	Media Storage	**Primary**: A.10.7.1 A.10.7.2 A.10.7.3 A.10.7.4 A.15.1.3	

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
MP-5	Media Transport	**Primary**: A.9.2.5 A.9.2.7 A.10.8.3	
MP-6	Media Sanitization and Disposal	**Primary**: A.9.2.6 A.10.7.2	
	Physical and Environmental Protection		
PE-1	Physical and Environmental Protection Policy and Procedures	**Primary**: §4.2.1(b) §5.1 A.5.1.1 A.9.1.4 A.9.2.1 A.9.2.2 A.11.1.1 A.11.2.1 A.11.2.2 A.11.2.3 Secondary: §4.3.1 (c) A.10.1.1 A.15.1.1 A.15.2.1 A.15.3.1	
PE-2	Physical Access Authorizations	**Primary**: A.9.1.2 A.11.2.1 A.11.2.2 A.11.2.4	The A.11.2.x controls are the means by which physical access may be driven (e.g. PIV cards)
PE-3	Physical Access Control	**Primary**: A.9.1.1 A.9.1.2 A.11.2.1 A.11.2.2 A.11.2.4	Requires cf. with A.11 ctrls,re logical ctrls as related issues. See comment above.
PE-4	Access Control for Transmission Medium	**Primary**: A.9.1.3 A.9.2.2 A.9.2.3	Just spcfc implications of A.9.1.3
PE-5	Access Control for Display Medium	**Primary**: A.9.1.3	See note above
PE-6	Monitoring Physical Access	Secondary: A.9.1.2	The key element of PE-6 is the responding to incidents. A.9.1.2 does not address this in 27002 guidance, although response can be considered as a form of protection. Hence view that it is secondary, but not worthy of an extended control.
PE-7	Visitor Control	**Primary**: A.9.1.2	
PE-8	Access Records	**Primary**: A.9.1.2	
PE-9	Power Equipment and Power Cabling	**Primary**: A.9.2.3	
PE-10	Emergency Shutoff	**Primary**: A.9.2.1	
PE-11	Emergency Power	**Primary**: A.9.1.4 A.9.2.2	
PE-12	Emergency Lighting	**Primary**: A.9.2.2	

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
PE-13	Fire Protection	**Primary**: A.9.1.4 A.9.2.2	
PE-14	Temperature and Humidity Controls	**Primary**: A.9.2.2	
PE-15	Water Damage Protection	**Primary**: A.9.1.4	
PE-16	Delivery and Removal	**Primary**: A.9.1.6 Secondary: A.9.2.7 A.10.7.1	
PE-17	Alternate Work Site	**Primary**: §4.2	This is a scoping issue – an alternative site may be fully configured, requiring services, infrastructure, etc. Include those sites within the ISMS, they then have to be treated accordingly, through risk assessment etc. (and see SP53.AA.x)
PE-18	Location of Information System Components	**Primary**: A.9.2.1	
PE-19	Information Leakage	**Primary**: A.12.5.4	NB – A.12.5.4 is much broader but embraces the concept, since EM emanations present a form of leakage/covert channel. Assume therefore an additional example as such under 27002 guidance.
		Planning	
PL-1	Security Planning Policy and Procedures	**Primary**: §4.2 §4.3.1(a) A.5.1.1 A.6.1.1 A.6.1.2 A.6.1.3 A.6.1.4 A.6.1.5 A.6.1.6 A.6.1.7 A.6.1.8 Secondary: A.10.1.1 A.15.1.1 A.15.2.1	
PL-2	System Security Plan	**Primary**: §4.2.1 §4.2.2 Secondary: A.15.2.1	Essentially 27001 conformity, hence A.15.2.1. PL-1 is more about process than controls *per se*
PL-3	System Security Plan Update	**Primary**: §4.2.3 §4.2.4 A.15.2.1	Essentially 27001 conformity, hence A.15.2.1. PL-1 is more about process than controls *per se*
PL-4	Rules of Behavior	**Primary**: A.7.1.3 A.8.1.1 A.8.1.3 A.15.1.5 Secondary: [A.11.3.1] [A.11.3.2] [A.11.3.3] [A.11.5.4]	

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
PL-5	Privacy Impact Assessment	**Primary**: A.15.1.4	
PL-6	Security-Related Activity Planning	**Primary**: §4.3 §7.1 §7.2 §7.3 A.12.1.1 A.15.3.1 Secondary: A.12.5.2 A.12.5.3	Although §7.1 states "at least annually" it is a general ISMS requirement that whenever any significant change is planned to the mgt system *per se*: A.12.1.1 relates more to application/OS changes.
		Personnel Security	
PS-1	Personnel Security Policy and Procedures	**Primary**: §4.2.1(b) §5.1 A.5.1.1 A.8.1.1 Secondary: §4.3.1(c) A.10.1.1 A.15.1.1 A.15.2.1 A.15.3.1	
PS-2	Position Categorization	**Primary**: A.8.1.1 A.8.1.2	Risk designation requires knowledge of roles and responsibilities and should be within that overall scoping. Screening is the application of that risk designation, per PS-2: PS-1 only requires the establishment of criteria...
PS-3	Personnel Screening	**Primary**: A.8.1.2	
PS-4	Personnel Termination	**Primary**: A.8.1.3 A.8.3.1 A.8.3.2 A.8.3.3 A.11.2.1	27001 combines termination and re-assignment within a single control group (A.8.3)
PS-5	Personnel Transfer	**Primary**: A.8.1.3 A.8.3.1 A.8.3.2 A.8.3.3 A.11.2.1	
PS-6	Access Agreements	**Primary**: A.6.1.5 A.8.1.3 A.11.2.1 (e)	
PS-7	Third-Party Personnel Security	**Primary**: A.6.2.3 (f, n, o) A.8.1.1 A.8.2.1 A.8.2.2 A.11.2.1 Secondary: A.6.2.1 A.8.1.3	
PS-8	Personnel Sanctions	**Primary**: A.8.2.3 A.11.2.1 (e)	
		Risk Assessment	

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
RA-1	Risk Assessment Policy and Procedures	**Primary**: §4.2.1(b)(2, 3, 4) §4.2.1(c) §4.2.3(d) §4.3.1 §5.1 A.5.1.1 Secondary: §4.3.1(c) A.10.1.1 A.15.1.1 A.15.2.1 A.15.3.1	
RA-2	Security Categorization	**Primary**: §4.2.1(b)(2, 4) §4.2.1(h) §4.2.1(i) A.7.2.1	Re. §4.2.1(b(4)), Categorization leads to establishing criteria for risk evaluation; (h & i) should also be interpreted in that context.
RA-3	Risk Assessment	**Primary**: §4.2.1(d) §4.2.1(e) §4.2.1(f) §4.2.1(g) §4.2.2(a) §4.2.2(b) §4.2.2(c) A.6.2.1 Secondary: A.12.6.1	Noteworthy is that RA-3 makes no mention of the selection of controls (27001 A.4.2) to mitigate the assessed risks (nor other RA-n excepting RA-1).
RA-4	Risk Assessment Update	**Primary**: §4.2.3(b) §4.2.3(c) §4.2.3(d)	
RA-5	Vulnerability Scanning	**Primary**: A.12.6.1	
		System and Services Acquisition	
SA-1	System and Services Acquisition Policy and Procedures	**Primary**: §4.2.1(b) §5.1 A.5.1.1 A.6.2.1 A.10.3.1 A.12.1.1 Secondary: §4.3.1(c) A.10.1.1 A.15.1.1 A.15.2.1 A.15.3.1	NB – it is recommended that the 'SA' class of controls addresses 'development', not just acquisition alone. That said, 27001 does not address this area at all well, it is a common weakness.

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
SA-2	Allocation of Resources	**Primary**: §4.2.2(a) §4.2.2(g) §5.1(e) §5.2.1 §7.3 (d) A.5.1.2 A.10.2.2 A.10.3.1 A.14.1.1 A.15.3.1 Secondary: §4.2.2(a) §4.2.2(g) A.6.1.2 A.7.1.3 A.14.1.3 A.14.1.4 A.14.1.5	
SA-3	Life Cycle Support	Secondary: SP53.SA.3, A.12.1.1	Inadequately addressed in terms of a 'life-cycle' philosophy for system support (within the ISMS) – it could be part of A.10.3 e.g. A.12.1.1 is a weak match.
SA-4	Acquisitions	**Primary**: A.6.2.1 A.6.2.3 A.12.1.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4	
SA-5	Information System Documentation	**Primary** : §4.3.1(c) §4.3.2 Secondary: A.10.7.4 A.15.1.3	Note – observe the explicit distinction 27001 makes between documentation and records
SA-6	Software Usage Restrictions	**Primary**: A.10.4.1 A.10.4.2 A.15.1.2	
SA-7	User Installed Software	**Primary**: SP53.SA.2 Secondary: A.15.1.5	
SA-8	Security Engineering Principles	**Primary**: A.5.1.1 A.6.1.1 SP53.SA.1	
SA-9	External Information System Services	**Primary**: A.6.1.5 A.6.2.1 A.6.2.3 A.10.2.1 A.10.2.2 A.10.2.3 A.10.6.2 Secondary: A.6.2.2	

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
SA-10	Developer Configuration Management	**Primary**: A.12.5.1 A.12.5.2 A.12.5.3 Secondary: A.6.2.1 A.6.2.3 A.12.5.5	A.12.5.3 included because of the need to use a configured version as a basis for development; If the developer is an outside external part the A.6 controls and A.12.5.5 also apply.
SA-11	Developer Security Testing	**Primary**: A.12.5.1 A.12.5.2 A.12.5.3 Secondary: A.12.5.5	As SA-10, A.12.5.3 refers to testing in a similar context.
System and Communications Protection			
SC-1	System and Communications Protection Policy and Procedures	**Primary**: §4.2.1(b) §5.1 A.5.1.1 A.10.8.1 Secondary: §4.3.1(c) A.10.1.1 A.15.1.1 A.15.2.1 A.15.3.1	
SC-2	Application Partitioning	**Primary**: A.11.4.5 A.11.4.6 A.11.4.7	
SC-3	Security Function Isolation	**Primary**: A.11.4.5 A.11.4.6 A.11.4.7	
SC-4	Information Remnance	**Primary**: SP53.SC.1	
SC-5	Denial of Service Protection	**Primary**: A.10.8.4(a) A.11.5.5 A.13.2.1	
SC-6	Resource Priority	**Primary**: SP53.SC.2	Prioritizing resources reflects upon consideration of resource availability. That said, the wording suggests this is more about OS task scheduling than management of ISMS resources, which could be addressed by §4.2.2(g), §5.2.1, §7.3 (d), A.5.1.2 and A.10.3.1. These have not been formally mapped on the basis that the resource issue is of a distinctly different class. It could be asked whether SC-6 is at too deep a level for the ISMS to directly address (and maybe even for -53?)
SC-7	Boundary Protection	**Primary**: A.10.6.2 A.10.10.2 A.10.10.4 A.11.4.2 A.11.4.5 A.11.4.6 Secondary: A.10.10.1 A.13.1.1 A.13.1.2 A.13.2.1	

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
SC-8	Transmission Integrity	**Primary**: A.10.6.1 (c) A.10.6.2 A.10.8.1 (a c g) A.10.9.1 (a d e g j) A.11.4.2 A.12.3.1	
SC-9	Transmission Confidentiality	**Primary**: A.10.6.1 (c) A.10.6.2 A.10.8.1 (a c g) A.10.9.1(d f g j) A.10.9.2 (b c) A.11.4.2 A.12.3.1	
SC-10	Network Disconnect	**Primary**: A.11.5.5 A.11.5.6	
SC-11	Trusted Path	**Primary**: A.10.9.2	
SC-12	Cryptographic Key Establishment and Management	**Primary**: A.12.3.1 A.12.3.2	
SC-13	Use of Cryptography	**Primary**: A.12.3.1 A.12.3.2 A.15.1.6	Note – A.12.3.2 would have been considered inapplicable, other than in a recursive sense, but for the fact that it references to other applicable standards (see 'Other information' in 27002).
SC-14	Public Access Protections	**Primary**: A.10.7.4 (c, d) A.10.9.3 A.12.2.4	
SC-15	Collaborative Computing	WBC.1.3	
SC-16	Transmission of Security Parameters	**Primary**: A.7.2.1 A.7.2.2 A.10.8.2 A.10.9.2	
SC-17	Public Key Infrastructure Certificates	**Primary**: A.12.3.2	
SC-18	Mobile Code	**Primary**: A.10.4.2	
SC-19	Voice Over Internet Protocol	**Primary**: WBC.1.1, WBC.1.2	
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	**Primary**: SP53.SC.5	
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	**Primary**: SP53.SC.5	
SC-22	Architecture and Provisioning for Name/Address Resolution Service	**Primary**: SP53.SC.6	

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
SC-23	Session Authenticity	**Primary**: A.10.9.2 A.11.4.1 A.11.4.2	
		System and Information Integrity	
SI-1	System and Information Integrity Policy and Procedures	**Primary**: §4.2.1(b) §5.1 A.5.1.1 Secondary: §4.3.1(c) A.10.1.1 A.15.1.1 A.15.2.1 A.15.3.1	
SI-2	Flaw Remediation	**Primary**: §4.2.2(h) A.10.10.5 A.12.4.1 A.12.5.2 A.12.6.1 A.13.1.1 A.13.1.2 A.13.2.1 A.13.2.2	
SI-3	Malicious Code Protection	**Primary**: A.10.1.4 A.10.4.1 A.10.4.2 A.10.8.1 Secondary: A.6.2.3 A.9.1.5 A.11.6.1 A.11.7.1 A.12.5.5 A.13.2.1	
SI-4	Information System Monitoring Tools and Techniques	**Primary**: A.10.6.2 A.10.10.1 A.10.10.2 A.10.10.4 Secondary: A.13.1.1 A.13.1.2 A.13.2.1	Secondary controls are additional techniques, such as reporting, which supports monitoring at the management level, rather than the technical level.
SI-5	Security Alerts and Advisories	**Primary**: A.6.1.7 A.10.4.1 A.13.1.1 A.13.1.2 A.13.2.1	
SI-6	Security Functionality Verification	**Primary**: A.10.10.2 A.15.2.2	

800-53 CNTL NO.	CONTROL NAME	ISO/IEC 27001 ref(s)	Comments
SI-7	Software and Information Integrity	**Primary**: A.10.4.1 A.10.10.2 A.12.2.1 A.12.2.2 A.12.2.3 Secondary: A.10.8.5	
SI-8	Spam Protection	**Primary**: A.10.6.1 (c) A.11.7.1 Secondary: A.10.4.1	
SI-9	Information Input Restrictions	**Primary**: A.11.1.1 A.11.2.2 A.11.4.1 A.11.4.2 A.11.5.1 A.11.6.1 A.11.7.1 A.11.7.2 Secondary: A.12.2.1 A.12.2.2	A.12.2.1/2 *only if* input data is accepted subject to authentication of the person providing the input (SI-9 refers to input by '*authorized personnel*' – the 27001 controls are concerned with validation data in terms of its syntax and internal consistency, not its origin) – although this specific issue could be addressed as a '12.1.0'.
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	Primary: A.12.2.1 A.12.2.2	A.10.7.3 is about information outside of the processing components of the information system: SI-10 is more to do with the system itself
SI-11	Error Handling	**Primary**: A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.5.4 A.12.6.1	
SI-12	Information Output Handling and Retention	**Primary**: A.10.7.3 A.15.1.3 A.15.1.4 A.15.1.5 A.15.2.1 Secondary: A.5.1.1 A.5.1.2 A.12.2.4	SI-12 addresses handling and retention in accordance with various refs. Is validation considered to be handling? Suggest that latter is in this context more to do with how handled, i.e. by whom and for what purpose.

J.3 ISO/IEC 27001 + EXTENDED CONTROL SET ➔ SPECIAL PUBLICATION 800-53 MAPPING

Cautionary note

Any mapping in this table between Special Publication 800-53 Security Controls and any sub-clause in §4 to §8, inclusive, of ISO/IEC 27001 has to be taken as being a contributory mapping from the Security Control, since those controls are focused upon the information system, not the information security management system. For that reason, some ISO/IEC 27001 requirements are simply judged not to be adequately fulfilled by Special Publication 800-53, and in some case mappings are shown within square brackets, suggesting that there is a relationship, but it is more in spirit than in explicitly matching statements of control requirements. Thus, any ISMS implemented to show compliance with Special Publication 800-53 requirements will need to put in place specific measures to fulfil the needs of ISO/IEC 27001 and embrace the Special Publication 800-53 Security Controls.

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
§4	**Information security management system**	
§4.1	**General requirements**	
	ISMS documented and maintained	CA-1
§4.2	**Establishing and managing the ISMS**	PL-1
§4.2.1	**Establish the ISMS**	CA-1 PL-2
§4.2.1(a)	Scope of the ISMS defined	§3.3.2(f) §3.3.2(g)
§4.2.1(b)	Information Security policy defined	§3.1.1 §3.2 §3.3.1(a) §3.3.2(f) §3.3.2(g) §3.3.2(h) §3.3.3(a) §3.4.1 AC-1 AT-1 AU-1 CA-1 CA-5 CM-1 CP-1 IA-1 IR-1 MA-1 MP-1 PE-1 PS-1 RA-1 RA-2 SA-1 SC-1 SI-1 See also SP53.AA.2
§4.2.1(c)	Systematic approach to risk assessment defined	§3.1.1 §3.1.2 §3.1.3 §3.2 §3.3.1(a)

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
		§3.3.2(h) §3.3.3(a) §3.4.1 §3.4.2 §3.4.3 RA-1 See also SP53.AA.2
§4.2.1(d)	Risks identified	§3.1.3 §3.3.2(b) §3.3.2(c) §3.3.2(d) §3.3.2(e) §3.3.2(h) §3.3.3(a) §3.4.1 §3.4.2 §3.4.3 CM-8 RA-3
§4.2.1(e)	Risks identified and assessed	§3.1.3 §3.3.2(b) §3.3.2(c) §3.3.2(d) §3.3.2(e) §3.3.2(h) §3.3.3(a) §3.4.1 §3.4.2 §3.4.3 RA-3
§4.2.1(f)	Options for risk treatment identified and evaluated	§3.1.3 §3.3.2(b) §3.3.2(c) §3.3.2(d) §3.3.2(e) §3.3.2(h) §3.3.3(a) §3.3.4 §3.4.1 §3.4.2 §3.4.3 RA-3
§4.2.1(g)	Appropriate control objectives and controls selected	§3.1.2 §3.1.3 §3.3.1(b) §3.3.1(c) §3.3.2(b) §3.3.2(c) §3.3.2(d) §3.3.2(e) §3.3.2(h) §3.3.3(a) §3.3.4 §3.4.1 §3.4.2 §3.4.3 RA-3
§4.2.1(h)	Management approval of the proposed residual risks	§3.1.7 §3.3.1(c)

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
		§3.3.3(c) CA-4 RA-2
§4.2.1(i)	Management authorization to implement and operate the ISMS	§3.3.1(c) §3.3.3(b) CA-6 RA-2
§4.2.1(j)	Statement of Applicability prepared	§3.1.4 §3.1.7 §3.3.1(b) §3.3.1(c) §3.3.2(a) §3.3.2(b) §3.3.2(c) §3.3.2(d) §3.3.2(e) §3.3.3(b) §3.3.3(c) §3.3.4 §3.4.1 §3.4.2 §3.4.3 §3.4.4 See also SP53.AA.6
§4.2.2	**Implement and operate the ISMS**	§3.1.5 §3.5.1 CA-1 PL-2
§4.2.2(a)	Formulate a risk treatment plan	RA-3 SA-2
§4.2.2(b)	Implement the risk treatment plan	RA-3
§4.2.2(c)	Implement the selected controls	§3.1.5 RA-3
§4.2.2(d)	Define how to measure the effectiveness of controls	[§3.5.2(c) – no explicit requirement to define how. Similar refs. in §1.1, and other parts of §1, in §2.5.] See also SP53.AA.1
§4.2.2(e)	Implement training and awareness programmes	IR-2
§4.2.2(f)	Manage operation of the ISMS	[§3.1 – the caveat is that this is focused on risk management for the specific info. system, not a broader ISMS approach]
§4.2.2(g)	Manage resources for the ISMS	SA-2 SC-6
§4.2.2(h)	Procedures to detect and respond to security events and incidents	SI-2
§4.2.3	**Monitoring and review the ISMS**	§3.1.6 §3.1.8 §3.5.1 §3.5.2(a) §3.5.2(b) §3.5.2(c) AU-6 CA-1 CA-7 PL-3

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
§4.2.3(a)	Execute monitoring and reviewing procedures and controls	AU-6
§4.2.3(b)	Undertake regular reviews of the effectiveness of the ISMS	AU-6 RA-4
§4.2.3(c)	Measure the effectiveness of controls	RA-4
§4.2.3(d)	Review the risk assessment and residual risk accounting for changing factors	AC-14 AU-6 RA-1 RA-4
§4.2.3(e)	Regularly-planned internal audits	AU-1
§4.2.3(f)	Management review of scope and identification of improvements	Considered ISMS-specific
§4.2.3(g)	Updating security plans to account for monitoring and review outcomes	Considered ISMS-specific
§4.2.3(h)	Record actions and events that could impair performance or effectiveness of the ISMS	Considered ISMS-specific
§4.2.4	**Maintaining and improving the ISMS**	§3.5.1 §3.5.2(a) §3.5.2(b) §3.5.2(c) CA-1 PL-3
§4.2.4(a)	Implement improvements	Considered ISMS-specific
§4.2.4(b)	Take actions to continually improve the ISMS	Considered ISMS-specific
§4.2.4(c)	Communicate and agree improvement actions	Considered ISMS-specific
§4.2.4(d)	Ensure that improvements fulfill the intention	Considered ISMS-specific
§4.3	**Documentation requirements**	PL-1 PL-6
§4.3.1	**General** Evidence of established and documented management framework	
§4.3.1(a)	Statements of policy and objectives	§3.3.4 §3.4.1 §3.4.2 §3.4.3 PL-1
§4.3.1(b)	Scope	§3.3.4 §3.4.1 §3.4.2 §3.4.3
§4.3.1(c)	Procedures and controls	AC-1 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IR-1 MA-1 MP-1 PE-1 PS-1 RA-1 SA-1

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
		SC-1 SI-1 SA-5
§4.3.1(d)	Risk assessment methodology	Driven by other NIST publications
§4.3.1(e)	Risk assessment report	Driven by other NIST publications
§4.3.1(f)	Risk treatment plan	Driven by other NIST publications
§4.3.1(g)	Procedures to ensure the effective planning, operation and control of its information security processes	QED, by compliance with NIST publications?
§4.3.1(h)	Records required by ISO/IEC 27001:2005	AU-11
§4.3.1(i)	Statement of Applicability	§3.1.4 §3.1.7 §3.3.1(b) §3.3.1(c) §3.3.2(a) §3.3.2(b) §3.3.2(c) §3.3.2(d) §3.3.2(e) §3.3.3(b) §3.3.3(c) §3.3.4 §3.4.1 §3.4.2 §3.4.3 §3.4.4
§4.3.2	**Control of documents** Procedures established and maintained for protection and control of all documentation required by the ISMS	CA-7 SA-5
§4.3.3	**Control of records** ▪ Records maintained to demonstrate compliance with ISO/IEC 27001:2005. ▪ Records legible, identifiable and traceable to the activity involved. ▪ Records stored and maintained in such a way that they are readily retrievable and protected against damage, deterioration or loss.	AT-4 AU-7 AU-8 AU-9 AU-11
§5	**Management responsibility**	§3.4.3
§5.1	**Management commitment**	
	Management must provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS	AC-1 AT-1 AU-1 CA-1 CA-5 CM-1 CP-1 IA-1 IR-1 MA-1 MP-1

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
		PE-1 PS-1 RA-1 RA-2 SA-1 SC-1 SI-1
§5.1(a)	Establishing an information security policy	Implicitly from §5.1 mappings
§5.1(b)	Ensuring that information security objectives and plans are established	Implicitly from §5.1 mappings
§5.1(c)	Establishing roles and responsibilities for information security	Implicitly from §5.1 mappings
§5.1(d)	Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement	Implicitly from §5.1 mappings
§5.1(e)	Providing sufficient resources to develop, implement, operate and maintain the ISMS	Implicitly from §5.1 mappings SA-2
§5.1(f)	Deciding the risk acceptance criteria and the acceptable level of risk	Implicitly from §5.1 mappings
§5.1(g)	Ensuring that internal ISMS audits are conducted	Implicitly from §5.1 mappings
§5.1(h)	Conducting management reviews of the ISMS	Implicitly from §5.1 mappings CP-5
§5.2	**Resource management**	
§5.2.1	**Provision of resources**	AU-4 SA-2 SC-6
§5.2.2	**Training, awareness and competence**	AT-1 AT-2 AT-3 AU-1 CP-3 IR-2
§6	**Internal ISMS audits**	§3.1.6 §3.1.8 AU-1 AU-6 CA-2 CA-6 CA-7
§7	**Management review of the ISMS**	§3.1.6 §3.1.8 §3.5.1 §3.5.2(a) §3.5.2(b) §3.5.2(c) AU-6
§7.1	**General**	AU-6 CA-5 CA-7 CP-5 PL-6

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
§7.2	**Review input**	AU-6 CA-5 CA-7 CP-5 PL-6
§7.3	**Review output**	§3.4.4 AU-6 CA-5 CA-7 CP-5 PL-6 SA-2 SC-6
§8	**ISMS improvement**	§3.5.1 §3.5.2(a) §3.5.2(b) §3.5.2(c)
§8.1	**Continual Improvement**	Implicitly from §8 mappings
§8.2	**Corrective Action**	Implicitly from §8 mappings
§8.3	**Preventive Action**	Implicitly from §8 mappings

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
A.5	**SECURITY POLICY**	
A.5.1	***INFORMATION SECURITY POLICY***	§3.4.3(a)
A.5.1.1	Information security policy document	AC-1 CA-1 CA-4 CM-1 CP-1 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1 PS-1 RA-1 SA-1 SC-1 SI-1 SI-12
A.5.1.2	Review of the information security policy	AC-1 CA-1 CA-5 CM-1 CP-1 IR-1 SA-2 SC-6 SI-12
A.6	**ORGANIZATION OF INFORMATION SECURITY**	

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
A.6.1	***INTERNAL ORGANIZATION***	
A.6.1.1	Management commitment to information security	AU-4 IA-1 PL-1 SA-8
A.6.1.2	Information security co-ordination	PL-1 SA-2
A.6.1.3	Allocation of information security responsibilities	AC-1 PL-1
A.6.1.4	Authorization process for information processing facilities	CA-3 PL-1
A.6.1.5	Confidentiality agreements	AC-13 AC-20 PL-1PS-6 SA-9
A.6.1.6	Contact with authorities	IR-6 PL-1
A.6.1.7	Contact with special interest groups	AT-5 PL-1 SI-5
A.6.1.8	Independent review of information security	CA-2 PL-1
A.6.2	***EXTERNAL PARTIES***	
A.6.2.1	Identification of risks related to external parties	AC-8 AC-20 CA-3 CP-6 CP-7 PS-7 RA-3 SA-1 SA-4 SA-9 SA-10
A.6.2.2	Addressing security when dealing with customers	AC-2 AC-8 AC-13 AC-20 CA-3 CP-6 CP-7 SA-9
A.6.2.3	Addressing security in third party agreements	AC-2 AC-13 AC-20 CA-3 CP-6 CP-7 PS-7 SA-4 SA-9 SA-10 SI-3
A.7	**ASSET MANAGEMENT**	§3.4.3 §3.4.3(a) §3.4.3(c) See also SP53.AA.1

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
A.7.1	***RESPONSIBILITY FOR ASSETS***	
A.7.1.1	Inventory of assets	CA-7 CM-2 CM-8 See also SP53.CM.1
A.7.1.2	Ownership of assets	CA-7 CM-8 See also SP53.CM.1
A.7.1.3	Acceptable use of assets	AC-20 CA-7 PL-4 SA-2
A.7.2	***INFORMATION CLASSIFICATION***	
A.7.2.1	Classification guidelines	AC-15 AC-16 RA-2 SC-16
A.7.2.2	Information labeling and handling	AC-15 AC-16 MP-3 SC-16
A.8	**HUMAN RESOURCES SECURITY**	
A.8.1	***PRIOR TO EMPLOYMENT***	
A.8.1.1	Roles and responsibilities	AC-1 AC-8 AC-20 AT-1 AU-1 PL-4 PS-1 PS-2 PS-7
A.8.1.2	Screening	PS-2 PS-3
A.8.1.3	Terms and conditions of employment	AC-8 AC-20 PL-4 PS-4 PS-5 PS-6 PS-7
A.8.2	***DURING EMPLOYMENT***	
A.8.2.1	Management responsibilities	AT-2 AT-3 PS-7
A.8.2.2	Information security awareness, education and training	AT-2 AT-3 CP-3 IR-2 PS-7
A.8.2.3	Disciplinary process	PS-8
A.8.3	***Termination or change of employment***	

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
A.8.3.1	Termination responsibilities	PS-4 PS-5
A.8.3.2	Return of assets	PS-4 PS-5
A.8.3.3	Removal of access rights	AC-2 PS-4 PS-5
A.9	**PHYSICAL AND ENVIRONMENTAL SECURITY**	§3.3.2(b) §3.3.2(c) §3.3.2(d) §3.3.2(e) §3.4.3(a)
A.9.1	***SECURE AREAS***	
A.9.1.1	Physical security perimeter	AC-1 PE-3
A.9.1.2	Physical entry controls	AC-1 AC-3 AC-13 PE-2 PE-3 PE-6 PE-7 PE-8
A.9.1.3	Securing offices, rooms and facilities	AC-1 PE-4 PE-5
A.9.1.4	Protecting against external and environmental threats	PE-1 PE-11 PE-13 PE-15
A.9.1.5	Working in secure areas	SI-3
A.9.1.6	Public access, delivery and loading areas	AC-3 PE-16
A.9.2	***EQUIPMENT SECURITY***	
A.9.2.1	Equipment siting and protection	AC-3 PE-1 PE-10 PE-18
A.9.2.2	Supporting utilities	PE-1 PE-4 PE-11 PE-12 PE-13 PE-14
A.9.2.3	Cabling security	PE-4 PE-9
A.9.2.4	Equipment maintenance	MA-2 MA-3 MA-6
A.9.2.5	Security of equipment off-premises	AC-20 MP-5
A.9.2.6	Secure disposal or re-use of equipment	MP-6
A.9.2.7	Removal of Property	AC-20 CA-7 MP-5

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
		PE-16
A.10	**COMMUNICATIONS AND OPERATIONS MANAGEMENT**	§3.3.2(e) §3.4.3(a)
A.10.1	***OPERATIONAL PROCEDURES AND RESPONSIBILITIES***	
A.10.1.1	Documented operating procedures	AC-1 AT-1 AU-1 CA-1 CM-1 CM-3 CP-1 IA-1 IR-1 MA-1 MP-1 PE-1 PL-1 PS-1 RA-1 SA-1 SC-1 SI-1
A.10.1.2	Change management	CA-7 CM-3
A.10.1.3	Segregation of duties	AC-5
A.10.1.4	Separation of development, test and operational facilities	SI-3
A.10.2	***THIRD PARYY SERVICE DELIVERY MANAGEMENT***	
A.10.2.1	Service delivery	CP-8 SA-9 See also SP53.CP.1
A.10.2.2	Monitoring and review of third party services	AC-13 AU-2 SA-2 SA-9
A.10.2.3	Managing changes to third party services	CM-3 SA-9
A.10.3	***SYSTEM PLANNING AND ACCEPTANCE***	
A.10.3.1	Capacity management	AU-4 SA-1 SA-2 SC-6
A.10.3.2	System acceptance	CA-4 CA-6
A.10.4	***PROTECTION AGAINST MALICIOUS AND MOBILE CODE***	
A.10.4.1	Controls against malicious code	AC-19 SA-6 SI-3 SI-5 SI-7 SI-8
A.10.4.2	Controls against mobile code	AC-19 SA-6 SC-18

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
		SI-3
A.10.5	***BACK-UP***	
A.10.5.1	Information Back-up	CP-4 CP-6 CP-9
A.10.6	***NETWORK SECURITY MANAGEMENT***	
A.10.6.1	Network controls	AC-5 AC-13 AC-18 SC-8 SC-9 SI-8
A.10.6.2	Security of network services	AC-4 SA-9 SC-7 SC-8 SC-9 SI-4
A.10.7	***MEDIA HANDLING***	
A.10.7.1	Management of removable media	MP-1 MP-2 MP-4 PE-16
A.10.7.2	Disposal of media	MP-1 MP-4 MP-6
A.10.7.3	Information handling procedures	AC-3 MP-1 MP-2 MP-3 MP-4 SI-12
A.10.7.4	Security of system documentation	MP-1 MP-4 SA-5 SC-14
A.10.8	***EXCHANGE OF INFORMATION***	
A.10.8.1	Information exchange policies and procedures	AC-18 SC-1 SC-8 SC-9 SI-3 See also SP53.SC.1
A.10.8.2	Exchange agreements	MP-3 SC-16
A.10.8.3	Physical media in transit	MP-5
A.10.8.4	Electronic messaging	SC-5
A.10.8.5	Business information systems	SI-7
A.10.9	***ELECTRONIC COMMERCE SERVICES***	
A.10.9.1	Electronic commerce	AU-10 SC-8 SC-9

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
A.10.9.2	On-line transactions	SC-9 SC-11 SC-16 SC-23
A.10.9.3	Publicly-available information	SC-14
A.10.10	***MONITORING***	
A.10.10.1	Audit logging	AC-5 AC-13 AU-3 AU-11 SC-7 SI-4
A.10.10.2	Monitoring system use	AC-13 AU-6 SC-7 SI-4 SI-6 SI-7
A.10.10.3	Protection of log information	AU-4 AU-5 AU-7 AU-9
A.10.10.4	Administrator and operator logs	AC-13 AU-2 AU-3 AU-6 SC-7 SI-4
A.10.10.5	Fault logging	SI-2
A.10.10.6	Clock synchronization	AU-2 AU-8
A.11	**ACCESS CONTROL**	§3.3.2(e) §3.4.3(a) §3.4.3(c)
A.11.1	***BUSINESS REQUIREMENT FOR ACCESS CONTROL***	
A.11.1.1	Access control policy	AC-1 AC-6 AC-14 AC-17 AC-18 AC-19 AU-10 CM-5 IA-1 IA-4 MP-1 PE-1 SI-9
A.11.2	***USER ACCESS MANAGEMENT***	§3.4.3 CM-5
A.11.2.1	User registration	AC-1 AC-2 AC-5

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
		AU-10 IA-1 IA-2 IA-4 PE-1 PE-2 PE-3 PS-4 PS-5 PS-6 PS-7 PS-8
A.11.2.2	Privilege management	AC-1 AC-2 AC-3 AC-6 AU-10 PE-1 PE-2 PE-3 SI-9
A.11.2.3	User password management	AC-1 AC-2 PE-1
A.11.2.4	Review of user access rights	AC-1 AC-2 PE-2 PE-3
A.11.3	***USER RESPONSIBILITIES***	
A.11.3.1	Password use	IA-5 [PL-4]
A.11.3.2	Unattended user equipment	[PL-4]
A.11.3.3	Clear desk and clear screen policy	[PL-4]
A.11.4	***NETWORK ACCESS CONTROL***	§3.4.3(b)
A.11.4.1	Policy on use of network services	AC-1 AC-17 AU-10 SC-23 SI-9
A.11.4.2	User authentication for external connections	AC-3 AC-4 AC-17 AC-18 AU-10 CA-3 IA-2 SC-7 SC-8 SC-9 SC-23 SI-9
A.11.4.3	Equipment identification in networks	AC-3 AC-4 AC-17 AC-19

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
		IA-3
A.11.4.4	Remote diagnostic and configuration port protection	AC-4 AC-17 MA-4
A.11.4.5	Segregation in networks	AC-4 AC-17 AC-18 SC-2 SC-3 SC-7
A.11.4.6	Network connection control	AC-3 AC-4 AC-17 SC-2 SC-3 SC-7
A.11.4.7	Network routing control	AC-4 AC-17 SC-2 SC-3
A.11.5	***OPERATING SYSTEM ACCESS CONTROL***	
A.11.5.1	Secure log-on procedures	AC-2 AC-7 AC-12 AU-10 SI-9 See also SP53.IA.2
A.11.5.2	User identification and authentication	AC-2 AC-3 AU-10 IA-2 IA-5
A.11.5.3	Password management system	IA-2 IA-5
A.11.5.4	Use of system utilities	[PL-4]
A.11.5.5	Session time-out	AC-2 AC-11 AC-12 SC-5 SC-10
A.11.5.6	Limitation of connection time	AC-2 SC-10
A.11.6	***APPLICATION AND INFORMATION ACCESS CONTROL***	
A.11.6.1	Information access restriction	AC-1 CM-5 SI-3 SI-9
A.11.6.2	Sensitive system isolation	AC-3
A.11.7	***MOBILE COMPUTING AND TELEWORKING***	
A.11.7.1	Mobile computing and communications	AC-1 AC-17 AC-18 AC-19

Clause/ Control	Requirement/ Control Objective	Mapped SP 800-53 clause(s)
		AC-20 AT-2 AT-3 IA-3 SI-3 SI-8 SI-9
A.11.7.2	Teleworking	AC-1 AC-2 AC-4 AC-13 AC-17 AC-18 AU-2 SI-9
A.12	**Information systems acquisition, development and maintenance**	§3.3.2(e)
A.12.1	***Security requirements of information systems***	
A.12.1.1	Security requirements analysis and specification	CM-3 PL-6 SA-1 SA-3 SA-4
A.12.2	***Correct processing in applications***	
A.12.2.1	Input data validation	SA-4 SI-7 SI-9 SI-10 SI-11
A.12.2.2	Control of internal processing	SA-4 SI-7 SI-9 SI-10 SI-11
A.12.2.3	Message integrity	SA-4 SI-7 SI-11
A.12.2.4	Output data validation	SA-4 SC-14 SI-11 SI-12
A.12.3	***Cryptographic controls***	
A.12.3.1	Policy on the use of cryptographic controls	AC-17 AU-10 SC-8 SC-9 SC-12 SC-13
A.12.3.2	Key management	AC-17 SC-12 SC-13 SC-17
A.12.4	***Security of system files***	

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
A.12.4.1	Control of operational software	AU-2 CM-1 CM-3 SI-2
A.12.4.2	Protection of system test data	[AC-3 AC-4 - these are a part of the solution to this ISMS requirement but by no means all of it. No explicit 800-53 mapping]
A.12.4.3	Access control to program source code	MA-5
A.12.5	***SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES***	§3.5.1 §3.5.2
A.12.5.1	Change control procedures	CA-7 CM-1 CM-2 CM-3 MA-2 MA-5 SA-10 SA-11
A.12.5.2	Technical review of applications after operating system changes	CA-7 CM-3 CM-4 MA-2 PL-6 SA-10 SA-11 SI-2
A.12.5.3	Restrictions on changes to software packages	CA-7 CM-1 CM-3 CM-5 MA-2 PL-6 SA-10 SA-11
A.12.5.4	Information leakage	PE-19 SI-11
A.12.5.5	Outsourced software development	SA-10 SA-11 SI-3
A.12.6	***TECHNICAL VULNERABILITY MANAGEMENT***	
A.12.6.1	Control of technical vulnerabilities	AU-2 RA-3 RA-5 SI-2 SI-11
A.13	**INFORMATION SECURITY INCIDENT MANAGEMENT**	§3.5.1 §3.5.2 §3.5.2(a) §3.5.2(b) §3.5.2(c)
A.13.1	***REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES***	
A.13.1.1	Reporting information security events	IR-1 IR-6

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
		SC-7 SI-2 SI-4 SI-5
A.13.1.2	Reporting security weaknesses	IR-7 SC-7 SI-2 SI-4 SI-5
A.13.2	***MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS***	
A.13.2.1	Responsibilities and procedures	AC-13 AU-2 AU-5 IR-4 SC-5 SC-7 SI-2 SI-3 SI-4 SI-5
A.13.2.2	Learning from information security incidents	IR-5 SI-2
A.13.2.3	Collection of evidence	AU-3 AU-9 AU-11
A.14	**BUSINESS CONTINUITY MANAGEMENT**	
A.14.1	***INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT***	
A.14.1.1	Including information security in the business continuity management process	CP-1 CP-5 CP-8 SA-2 See also SP53.CP.1
A.14.1.2	Business continuity and risk assessment	CP-1 CP-2
A.14.1.3	Developing and implementing continuity plans including information security	CP-2 CP-6 CP-7 SA-2
A.14.1.4	Business continuity planning framework	CP-2 CP-3 CP-6 CP-7 SA-2
A.14.1.5	Testing, maintaining and re-assessing business continuity plans	CP-4 CP-5 CP-6 CP-7 IR-3 SA-2
A.15	**COMPLIANCE**	§3.1.8 §3.3.2(e) §3.3.4
A.15.1	***COMPLIANCE WITH LEGAL REQUIREMENTS***	§3.3.2(f)

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
A.15.1.1	Identification of applicable legislation	AC-1 AC-10 AT-1 AU-1 CA-1 CM-1 CP-1 IA-1 IA-7 IR-1 MA-1 MP-1 PE-1 PL-1 PS-1 RA-1 SA-1 SC-1 SI-1
A.15.1.2	Intellectual property rights (IPR)	SA-6
A.15.1.3	Protection of organizational records	AU-9 AU-11 MP-1 MP-3 MP-4 SA-5 SI-12
A.15.1.4	Data protection and privacy of personal information	AC-8 CP-1 PL-5 SI-12
A.15.1.5	Prevention of misuse of information processing facilities	AC-2 AC-8 PL-4 SA-7 SI-12
A.15.1.6	Regulation of cryptographic controls	AC-17 IA-7 SC-13
A.15.2	***COMPLIANCE WITH SECURITY POLICIES AND STANDARDS AND TECHNICAL COMPLIANCE***	
A.15.2.1	Compliance with security policies and standards	AC-1 AT-1 AU-1 CA-1 CA-2 CM-1 CP-1 IA-1 IA-7 IR-1 MA-1 MP-1 PE-1 PL-1 PL-2 PL-3

CLAUSE/ CONTROL	REQUIREMENT/ CONTROL OBJECTIVE	MAPPED SP 800-53 CLAUSE(S)
		PS-1 RA-1 SA-1 SC-1 SI-1 SI-12
A.15.2.2	Technical compliance checking	CA-2 SI-6
A.15.3	***INFORMATION SYSTEMS AUDIT CONSIDERATIONS***	§3.3.2(f)
A.15.3.1	Information systems audit controls	AC-13 AU-6 AT-1 AU-1 AU-2 CA-1 CM-1 CP-1 IA-1 IR-1 PE-1 PL-6 PS-1 RA-1 SA-1 SA-2 SC-1 SI-1
A.15.3.2	Protection of information systems audit tools	AU-7 AU-9

J.4 SPECIAL PUBLICATION 800-53 EXTENDED CONTROL SET

In the following table an Extended Control Set (ECS) is described. The controls defined should be added to the ISO/IEC 27001 Annex A reference controls so as to create the basis of an SoA which will ensure 100% SP 800-53 compliance-mapping capability through an ISMS. For compatibility purposes the controls are set out in a style closely following that used for the ISO/IEC 27001 controls in Annex A of that standard.

The ECS is described in normative terms so as to have normative value when used to extend an ISMS SoA, but in addition, Guidance is also given, following the Control objective. Where the Extended Control is derived directly from an SP 800-53 Security Control, the guidance refers simply to that control's identifier. Otherwise appropriate guidance is given directly with the Control specification.

Study of this ECS will show that care should be taken to ensure that within the ISMS the specific compliance of each included information system can be able to be readily determined and demonstrated. Where systems are widely different, for whatever reason, a single ISMS which embraces them all may not be efficient to operate. Organizations are therefore advised to consider carefully matters of ISMS scoping. It may prove to be more efficient to have two (or more) ISMSs and allow some parts of the management infrastructure to be present in each (with adequate risk assessment to ensure that controls are in place to protect the ISMS and systems within from one another.)

SP53	**Extended Control Set to support complete SP 800-53 ISMS SoA compliance mapping**	
SP53.AA	**Addressability of all information systems** *Objective*: to ensure that, within an ISMS which includes more than one system subject to FISMA, the applied ISMS policies, processes and controls address all of the systems so as to ensure that FISMA compliance is demonstrable. *Note*: This group of controls does not map into the FISMA Security Controls – these extended controls are necessary to facilitate, within the ISMS, the fulfillment of FISMA requirements at the individual information system level.	
SP53.AA.1	Individual System Identification	*Control* Where the ISMS has more than one information system falling within its scope the asset register shall identify those discrete systems and either assign assets as belonging to a specific system or indicate that they are common or shared, as applicable. *Guidance* The scope of an ISMS may embrace one or more information systems. Since FISMA addresses primarily individual information systems it requires risk assessments to be performed for each system within the scope of the ISMS (SP 800-53 / FIPS 200 / SP 800-30). A pre-requisite is that assets belonging to each system be specifically identified amongst the assets within the ISMS. This has a bearing upon the ISMS requirement in §4.2.2(d) and controls in control group A.7.
SP53.AA.2	Individual System Categorization and Minimum Assurance	*Control* The organization shall establish the security categorization and minimum assurance requirements for each information system falling within the scope of the ISMS. *Guidance* This control should be considered to be supplementary to §4.2.1(b) & §4.2.1(c). The scope of an ISMS may embrace one or more information systems. Since FISMA addresses primarily individual information systems it requires risk assessments to be performed for each system within the scope of the ISMS (SP 800-53 / FIPS 200 / SP 800-30). A pre-requisite is that the security category (FIPS 199 / SP 800-60) and the minimum assurance requirements (SP 800-53 App. E) for each system be assessed

		and determined in order to support the risk analysis.
SP53.AA.3	Individual System Risk Assessment	*Control* Risk assessments shall be performed for each system within scope of the ISMS. Where a risk assessment is common to two or more (or all) systems within scope it shall be clearly stated which systems are included. *Guidance* The scope of an ISMS may embrace one or more information systems. FISMA requires that each Federal information system (and those of contractors and suppliers) is compliant with SP 800-53. Risk assessment therefore needs to be shown to be performed for each explicit information system within scope of the ISMS, either individually or for two or more information systems, where the systems are such that they may be treated under the same assessment. Where two or more information systems are subject to the same risk assessment they may be of the same or different Security Categorizations (FIPS 199 / FIPS 200 / SP 800-53 / SP 800-60), but should be assessed at 'system high' (i.e. at the highest categorization level of all systems under a single risk assessment), where they differ. Common risk assessment may be a cost-effective way to include multiple information systems within an ISMS where they have similar security categorizations and share other characteristics.
SP53.AA.4	System-specific policy	*Control* Where information security (management) policies (or elements thereof) are specific to one or more discrete system(s) within scope of the ISMS there shall be a clear indication which are the systems affected and how they relate to the overall ISMS policies. *Guidance* The scope of an ISMS may embrace one or more information systems. System-specific policy is more likely to focus on technical aspects of the system within the broader scope of the ISMS' management-level policies. This will be particularly so where there is a policy- or risk-based need to deal with systems separately (e.g. where they have different security classifications/categorizations, where they are separated for security reasons such as being alternate resources, or where they provide services for specific clients or organizational functions.) There may be alternativelcost-based arguments for having separate information systems subject to the same policy/ies. System owners should justify this as a part of their risk assessment.
SP53.AA.5	System-specific documentation, controls and records	*Control* Each system shall be addressed by all applicable controls within the ISMS and policies, procedures etc. shall be clearly related to a specific system or group of systems, or be commonly applicable. *Guidance* The scope of an ISMS may embrace one or more information systems. In order to demonstrate FISMA compliance in respect of all SP 800-53 Security Controls it is essential that the ISMS can relate to specific documentation, controls and records required to operate each information system, even though some of those items may be at a lower level of granularity than the ISMS would normally address directly. Organizations using this ECS (SP53) should use its controls to map at the ISMS-level (of granularity) through to those SP 800-53 controls which extend into further levels of detail.
SP53.AA.6	System-focused Statement of Applicability	*Control* The organization shall prepare its Statement of Applicability such that it can be readily shown how each control applies to each information system within the scope of the ISMS. *Guidance* This control should be considered to be an extension of §4.2.1(j) as an additional item, "4) how each control applies to each information system within the scope of the ISMS." Since FISMA addresses primarily individual

		information systems it requires evidence of the compliance for each information system within the scope of the ISMS. Thus the ISMS must relate to each information system within its scope. Depending upon the degree to which the collective information systems share features, or are more disparate, will affect the extent to which security controls are commonly applied, allowing a common selection and implementation of controls, or at the other extreme, requiring individual responses within the SoA for each information system.
SP53.AU Audit and accountability policy & procedures *Objective*: To detect and provide evidence of unauthorized information processing activities		
SP53.AU.1	Audit synthesis and report generation	*Control* The system shall generate reports from audit logs without destroying their evidential value. *Guidance* Refer to SP 800-53 Security Control AU-7. Note – this control does not state explicitly that reports be summarized – only that (most importantly, in fact) they be produced without destroying the evidential value of the original logs. Whether reports are detailed or summarized is immaterial in a security (log integrity) context. *Drafting note – consider as the basis for an additional control for 27001, as A.10.10.7.*
SP53.CM *Objective*: To ensure that configuration management policy and procedures are in place to fully meet the FISMA requirements.		
SP53.CM.1	Baseline Configuration	*Control* The organization shall develop, document, and maintain a baseline configuration for each information system falling within the scope of the ISMS. *Guidance* This control should be considered to be a specific extension to A.7.1.1 and A.7.1.2, and is allied closely to SP53.AA.1. The scope of an ISMS may embrace one or more information systems and it is important that the organization maintains a record of the configuration for each of those systems within the ISMS which is accurate, reliable and up-to-date. Refer to SP 800-53 Security Control CM-2.
SP53.CM.2	Configuration Settings	*Control*. The organization shall establish, document, enforce and regularly review configuration settings for all information technology products employed within each information system falling within the scope of the ISMS. Configuration shall be the most restrictive consistent with operational requirements. *Guidance* Refer to SP 800-53 Security Control CM-6.
SP53.CM.3	Least Functionality	*Control*. The organization shall configure each information system falling within the scope of the ISMS such that it provides only essential capabilities. The use of functions, ports, protocols, and/or services not consistent with operational requirements shall be disabled. *Guidance* Refer to SP 800-53 Security Control CM-7.

SP53.CP *Objective*: To ensure that contingency planning policy and procedures are in place to fully meet the FISMA requirements.		
SP53.CP.1	Telecommunications Services	*Control*. The organization shall establish service agreements for primary telecommunications and alternate services to enable critical mission/business function continuity when the primary telecommunications capabilities are reduced or unavailable. Agreements shall address how services are switched between primary and alternate providers. *Guidance* This control should be seen as a specific instance of A.10.2.1 and/or A.14.1.1, each of which has a generic scope. Refer to SP 800-53 Security Control CP-8. *Drafting note – consider as the basis for an additional control for 27001.*
SP53.IA Identification and Authentication *Objective*: To ensure that identification and authentication mechanisms are in place to fully meet the FISMA requirements..		
SP53.IA.1	Credential Management	*Control* Credential management policies and procedures shall be documented, maintained and applied for each information system falling within the scope of the ISMS. The system shall address all aspects of the credential management life-cycle. *Guidance* Refer to SP 800-53 Security Control IA-1 and IA-5.
SP53.IA.2	Protection of authentication information	*Control* Measures shall be applied to protect against the use of authentication information by unauthorized individuals. *Guidance* This control should be considered as supplementary to A.11.5.1, placing attention on protection of the authentication data, whereas A.11.5.1 is focused on providing access control to the system. Furthermore, the ISMS usage is very focused on access to the **operating systems**, not so much to applications. Refer to SP 800-53 Security Control IA-6.
SP53.IR Management of information security incidents and improvements *Objective*: To ensure a consistent and effective approach is applied to the management of information security incidents.		
SP53.SA Systems and services acquisition *Objective*: To ensure that systems and services are acquired by means which fully meet the FISMA requirements..		
SP53.SA.1	Security Engineering Principles	*Control* System and service development procedures, addressing the whole life-cycle and based upon sound security engineering principles, shall be established, documented, maintained and made available to all users who need them. *Guidance* Refer to SP 800-53 Security Control SA-8. *Drafting note – consider as the basis for an additional control for 27001.*
SP53.SA.2	Control of user software installation	*Control* The organization shall establish and apply explicit rules governing the

(consider as A.12.6.2		installation of software by users. *Guidance* Refer to SP 800-53 Security Control SA-7. *Drafting note – consider as the basis for an additional control for 27001, as A.12.6.2.*
SP53.SA.3	Security in the development life-cycle	*Control* Information security shall be explicitly included within the system and service development life cycle methodology/ies. *Guidance* Refer to SP 800-53 Security Control SA-3. *Drafting note – consider as the basis for an additional control for 27001, as A.12.5.0.*
SP53.SC System and Communications Protection *Objective*: To ensure that system and communications protections are in place to fully meet the FISMA requirements. *Note*: These controls could collectively be considered to be a means of ensuring compliance with A.15.1.1 at the FISMA level and A.15.2.1 at the SP 800-53 level.		
SP53.SC.1	Information Remnance	*Control* Measures shall be applied to prevent unauthorized and unintended information transfer via shared information system resources.. *Guidance* Refer to SP 800-53 Security Control SC-4 and compare with ISO/IEC 27001 A.10.8.1 (which is not addressing the same issue).
SP53.SC.2	Resource Priority	*Control* Measures shall be applied to ensure that operating systems resources are allocated on a priority basis. *Guidance* Refer to SP 800-53 Security Control SC-6.
SP53.SC.3	Collaborative Computing	*Control* Unauthorized activation of collaborative computing mechanisms shall not be permitted. Users shall be given explicit indications that such mechanisms are in use. *Guidance* Refer to SP 800-53 Security Control SC-15.
SP53.SC.4	Not used	Moved to WBC.1
SP53.SC.5	Name /Address Resolution Service Authentication	*Control* Name/address resolution services shall authenticate all resolution queries they initiate and shall provide to local clients authentication credentials with all resolution queries requests to which they respond. *Guidance* Refer to SP 800-53 Security Controls SC-20 and SC-21
SP53.SC.6	Name /Address Resolution Service Fault Tolerance	*Control*. Name/address resolution services shall include redundancy and fault tolerant design. *Guidance* Refer to SP 80 0-53 Security Control SC-22.
WBC.1 Web-based Communications Protection (posited as revision to ISO/IEC 27001:2005, Annex A, as new controls under a new group, A.10.11 'Web-based communications')		

Objective: To ensure the security of web-based communication services.		
WBC.1.1	Authorized use of VoIP	*Control* The organization shall establish, document, apply and review an authorization process for the use of Voice over Internet Protocol (VoIP) services, including their monitoring and control. *Guidance* Refer to SP 800-53 Security Control SC-19.
WBC.1.2	Guidance on use of VoIP	*Control* Guidance on implementation and usage of Voice over Internet Protocol (VoIP) services shall be established, maintained and made available to all users who need them. *Guidance* should be Refer to SP 800-53 Security Control SC-19.
WBC.1.3	Collaborative computing management	*Control*. Access to collaborative computing services shall be actively controlled. *Guidance* Refer to SP 800-53 Security Control SC-15