NIST Special Publication 800-53

Recommended Security Controls for Federal Information Systems

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

Ron Ross
Gary Stoneburner
Stu Katzke
Arnold Johnson
Marianne Swanson
Annabelle Lee
George Rogers

I N F O R M A T I O N S E C U R I T Y

SECOND PUBLIC DRAFT

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

September 2004

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., 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 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.

Draft

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 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 A-130, Appendix III.

This guideline has been prepared for use by 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 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 official.

National Institute of Standards and Technology Special Publication 800-53, 94 pages

(September 2004) CODEN: NSPUE2

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

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. These include: NIST Special Publication 800-53A and FIPS 200. The methodologies in this document may be used even before the completion of the aforementioned companion documents. Thus, until such time as each is 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.

THE PUBLIC COMMENT PERIOD FOR THIS DOCUMENT BEGINS ON OCTOBER 1, 2004 AND ENDS ON NOVEMBER 30, 2004. COMMENTS MAY BE SUBMITTED TO THE COMPUTER SECURITY DIVISION, NIST, VIA ELECTRONIC MAIL AT SEC-CERT@NIST.GOV

OR VIA REGULAR MAIL AT

100 BUREAU DRIVE (MAIL STOP 8930)
GAITHERSBURG, MD 20899-8930

Acknowledgements

The authors, Ron Ross, Gary Stoneburner, Stu Katzke, Arnold Johnson, Marianne Swanson, Annabelle Lee, and George Rogers, wish to thank their colleagues who reviewed drafts of this document and contributed to its development. The authors also gratefully acknowledge and appreciate the many contributions from the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

Draft

Notes to Reviewers

The second public draft of NIST Special Publication 800-53 reflects the many significant changes in the document that resulted from the extensive feedback received from our customers during the initial public comment period and public workshop earlier this year. In the current draft, steps have been taken to simplify and clarify the security controls by introducing a new structure for the controls. The new structure includes: (i) a control section (describing the actual required security capability); (ii) a supplemental guidance section (providing additional details for control implementation); and (iii) a control enhancements section (listing additional security capabilities to strengthen controls, when needed).

In addition to simplifying the security controls and defining a new control structure, scoping guidance and minimum assurance requirements have been added to the current draft. The scoping guidance is intended to help organizations effectively apply the security controls in specific operational environments. The guidance addresses issues related to technology, infrastructure, common controls, and risk. The assurance requirements are intended to provide greater confidence to organizations that their security controls are effective—that is, 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.

Special Publication 800-53 has special significance in that the security controls contained in the recommended baselines will form the basis for those controls that will become mandatory in December 2005. At that time, Federal Information Processing Standard (FIPS) 200, *Minimum Security Controls for Federal Information Systems*, will take effect and be mandatory for federal agencies as required by FISMA. FIPS 200 will be applicable to all non-national security systems.

NIST invites the public to review and comment upon this guideline. We are interested in your feedback on: (i) the content of the individual security controls; (ii) the selection of security controls and control enhancements for the three baselines; and (iii) the cost and potential impact on organizations in employing such controls. Comments will be accepted through November 30th 2004. NIST will then revise the guideline and publish the final guideline in early 2005. Comments should be forwarded to the Computer Security Division, Information Technology Laboratory at NIST or submitted via email to sec-cert@nist.gov. The FISMA Implementation Project main web site at http://csrc.nist.gov/sec-cert contains information on all of the FISMA-related security standards and guidelines and how the publications can be used to manage enterprise risk and build a comprehensive information security program.

We have attempted to provide improvements in Special Publication 800-53 that will help our customers effectively select and specify security controls for their information systems—and to do so, using a risk-based approach that facilitates cost-effective information security. Your feedback to us, as always, is critical in the security standards and guidelines development process to ensure that the work products produced by NIST are meeting the security needs of the federal government and the constituencies in the private sector who voluntarily use those products.

-- RON ROSS
PROJECT LEADER, FISMA IMPLEMENTATION PROJECT

Table of Contents

Draft

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] is an important task that can have major implications on the operations[2] and assets of an organization. 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 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 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 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 ensure that information security is addressed throughout the life cycle of each organizational information system;
- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;

[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.

[2] Organizational operations include such things as 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 system.

[4] The E-Government Act (Public Law 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 information security for the information systems that support its operations and assets.

- 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 to ensure continuity of operations for information systems that support the operations and assets of the organization.

It is of paramount importance that responsible individuals within the organization understand the risks and other factors that could adversely affect their operations and assets. 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 missions 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 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 government. The guidelines have been developed to help achieve more secure information systems within the 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*;
- Promoting a dynamic, extensible catalog of security controls for information systems to meet the demands of 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 information systems other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542.[5] The guidelines have been broadly developed from a technical perspective so as to

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

be complementary to similar guidelines for national security systems. This publication is intended to provide guidance to federal agencies until the publication of FIPS 200, *Minimum Security Controls for Federal Information Systems* (projected for publication December 2005). State, local, and tribal governments, as well as private sector organizations composing the critical infrastructure of the United States, are encouraged to consider the use of these guidelines, as appropriate.

1.2 RELATIONSHIP TO OTHER SECURITY CONTROLS AND STANDARDS

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.[6] The objective of NIST Special Publication 800-53 is to provide a sufficiently rich set of security controls that satisfy the breadth and depth of security requirements[7] levied on information systems and that are 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[8] 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.

1.3 ORGANIZATIONAL RESPONSIBILITIES

Organizations should use FIPS 199 to define security categories for their information systems. The recommendations for minimum security controls from Special Publication 800-53 can subsequently be used as a starting point for and input to the organization's risk assessment[9] process and the development of security plans for those information systems. While the FIPS 199 security categorization associates the operation of the information system with the potential

[6] For example, security controls from the audit, defense, healthcare, intelligence, and standards communities are contained in the following publications: (i) General Accounting Office (GAO), *Federal Information System Controls Audit Manual*; (ii) Department of Defense (DoD) Instruction 8500.2, *Information Assurance Implementation*; (iii) Department of Health and Human Services (HHS) Centers for Medicare and Medicaid Services, *Core Security Requirements*; (iv) Director of Central Intelligence Directive (DCID) Manual 6/3, *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 (ISO/IEC) 17799:2000, *Code of Practice for Information Security Management.*

[7] 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.

[8] NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (projected for publication winter 2004-05), provides guidance on assessment methods and procedures for security controls defined in this publication.

[9] 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, and the process should be reasonable for the organization concerned. NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, provides guidance on the assessment of risk.

impact on an organization's operations and assets, the incorporation of refined threat and vulnerability information during the risk assessment process facilitates the tailoring of the baseline security controls to address organizational needs and tolerance for risk. Deviations from the recommended baseline security controls should be made in accordance with the scoping guidance provided in this special publication and documented with appropriate justification and supporting rationale in the security plan for the information system. The use of security controls from Special Publication 800-53 and the incorporation of baseline (minimum) controls as a starting point in the control selection process, facilitates a more consistent level of security in an organizational information system. It also offers the needed flexibility to tailor the controls based on specific organizational policy and requirements documents, particular conditions and circumstances, known threat and vulnerability information, or tolerance for risk to the organization's operations and assets.

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 component products; (iii) sound systems/security engineering principles and practices to effectively integrate component products into the information system; (iv) appropriate methods for product/system testing and evaluation; and (v) comprehensive system security planning and life cycle management. 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 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 *and* the cost, schedule, and performance issues associated with the acquisition, deployment, and operation of the system. In general, there may not be sufficient resources to satisfy all security, cost, schedule, and performance objectives for the information system. Organization officials should allocate resources appropriately in accordance with agreed-upon priorities and document the resource allocation decisions.

1.4 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter 2** 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) the use of common security controls in support of organization-wide information security programs; (iii) minimum security (baseline) controls; (iv) assurance in the effectiveness of security controls; and (v) the commitment to maintain currency of the individual security controls and the control baselines.
- **Chapter 3** describes the process of selecting and specifying security controls for an information system including: (i) the organization's overall approach to managing risk; (ii) the security categorization of the system and the selection of minimum (baseline) security controls; (iii) the activities associated with tailoring the baseline security controls; and (iv) the potential for supplementing the initial security control baselines, when required.
- **Supporting appendices** provide more detailed security control selection and specification-related information including: (i) general references; (ii) definitions and terms; (iii) acronyms; (iv) minimum security controls for low-, moderate-, and high-impact information systems; (v) minimum assurance requirements; (vi) catalog of security controls; and (vii) mapping tables relating the security controls in this publication to other standards and control sets.

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) the identification and use of common security controls; (iii) the application of minimum security controls, or control baselines, to information systems categorized in accordance with FIPS 199; (iv) security control assurance; and (v) 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 *families* for ease of use in the control selection and specification process. Each family contains security controls related to the security function of the family. A standardized, two-character identifier is assigned to uniquely identify each control family. Table 1 summarizes the families in the security control catalog and the family identifiers.

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

TABLE 1: SECURITY CONTROL FAMILIES AND IDENTIFIERS

To uniquely identify each control, a numeric identifier is appended to the family identifier to indicate the number of the control with 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. 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 how often it intends to conduct information system backups or how frequently it intends to test its contingency plan. 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. 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 should consider supplemental guidance when defining, developing, and implementing security controls. Applicable federal legislation, 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 additional statements of security capability needed to strengthen a basic control when the control is used in an information system requiring greater protection due to the potential impact of loss or when organizations seek additional control strength 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 following example from the Contingency Planning family illustrates the structure of a typical security control—that is, the basic control, the supplemental guidance for the control, and control enhancements. If the two control enhancements are selected, the control designation subsequently becomes CP-9 (1) (2).

CP-9 INFORMATION SYSTEM BACKUP

Control: The organization conducts [*Assignment: organization-defined time period*] backups of user-level and system-level information (including system state information) contained in the information system and stores backup information at an appropriately secured 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.

Control Enhancements:

(1) The organization tests backup information [*Assignment: organization-defined time period*] to ensure 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.

2.2 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 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.[10]

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, and information system security officers. The organization-wide exercise considers the classes of information systems within the organization in accordance with FIPS 199 (i.e., low-impact, moderate-impact, or high-impact systems) and the minimum security controls necessary to protect those systems (see *baseline* security controls in Section 2.3). For example, common security controls can be identified for all low-impact information systems by considering the baseline security controls for that class 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, and physical and environmental protection 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.

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

Information system owners are *not* responsible for the common security controls that are helping to protect their systems. They are, however, responsible for any system-specific issues associated with the implementation of those 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 assessment results are shared with the appropriate information system owners.

Partitioning security controls into common security controls and system-specific security controls can result in significant savings to the organization in control development and implementation costs. 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 dependence on common security controls by potentially 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.

2.3 SECURITY CONTROL BASELINES

Organizations must employ security controls to meet security requirements defined by laws, executive orders, directives, policies, 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 comply with the stated security requirements. 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 security categorization in accordance with FIPS 199.[11] Security categories derived from FIPS

[11] FIPS 199 security categories are based on the potential impact on an organization 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.

199 are typically considered during the risk assessment process to help guide the initial selection of security controls for an information system.[12] The risk assessment process provides useful information and a procedural approach to examining the important factors that ultimately determine which security controls are necessary to protect the organization's operations and assets. The baseline controls associated with the FIPS 199 security categories serve as a *starting point* for organizations in determining the appropriate safeguards and countermeasures necessary to protect their information systems. As the baselines are intended as broadly applicable starting points, modifications to the selected baseline may well be necessary in order to achieve adequate risk mitigation. Such modifications are tied to the risk assessment and documented in the security plan for the information system.

The complete catalog of security controls for information systems, arranged by control families, is provided in Appendix F. The catalog represents the entire set of security controls (defined at this time). From the control catalog, three sets of baseline security controls have been identified corresponding to the low-impact, moderate-impact, and high-impact levels defined in the security categorization process in FIPS 199. Appendix D provides a listing of the minimum security (baseline) controls associated with each of the FIPS 199 impact levels. Each of the three baselines provides a minimum set of security controls (or floor) for a particular impact level associated with a security category. Chapter 3 provides additional information on how to use security categories to select the appropriate set of baseline security controls.

Organizations or communities of interest may wish to demonstrate that the security controls selected for their information systems are sufficient to meet the security requirements defined in applicable federal legislation, executive orders, directives, policies, regulations, or standards. This can be accomplished by using what is commonly referred to as a requirements traceability matrix. The organization starts with the specific set of security requirements for which there must be compliance. Security requirements are mapped to appropriate security controls within the selected baseline of controls and the results documented.

2.4 SECURITY CONTROL ASSURANCE

Assurance is the grounds for confidence 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 of security controls to use state-of-the-practice 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.[13]

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 focus is on the control

[12] Security categories are used in conjunction with vulnerability and threat information in assessing the risk to an organization by operating an information system. FIPS 199 defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions takes place within the context of each organization and the overall national interest.

[13] NIST Special Publication 800-53A is projected for publication in the winter 2004-05.

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 focus is on ensuring 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 ensure the control meets its function or purpose. 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 to support continuous improvement in the control's effectiveness. There are additional assurance requirements available to developers and implementers supplementing the minimum assurance requirements for the high baseline in order to protect against threats from highly skilled, highly motivated, and well-financed threat agents. This level of protection is required for those information systems where the organization is not willing to accept the risks associated with the type of threat agents cited above.

2.5 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 revised and extended to reflect: (i) the experience gained from using the controls; (ii) the changing security requirements within organizations; and (iii) new security technologies that may be available. The controls populating the various families are expected to change over time, as controls are eliminated or revised and new controls are added. The proposed additions, deletions, or modifications to the catalog of security controls will go through a rigorous, public review process to obtain government and private sector feedback and to build consensus for the changes. The minimum security controls defined in the low, moderate, and high baselines are also expected to change over time as well, as the level of security and due diligence for mitigating risks within organizations increases. A dynamic, flexible, and technically rigorous set of security controls will be maintained in the control catalog to allow organizations and communities of interest to continue to be able to select the appropriate controls for their respective needs in a cost-effective manner.

Draft

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) the organization's overall approach to managing risk; (ii) the security categorization of the system in accordance with FIPS 199 and the selection of minimum (baseline) security controls; (iii) the activities associated with tailoring the baseline security controls through the application of scoping guidance and the assignment of organization-defined parameters; and (iv) the potential for supplementing the minimum security controls with additional controls, as necessary, to achieve adequate security.

3.1 MANAGING ORGANIZATIONAL 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 organizational risk—that is, the risk associated with the operation of an information system. The management of organizational 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 the operations and assets of the organization. Managing organizational risk includes several important activities: (i) assessing risk; (ii) conducting cost-benefit analyses; (iii) selecting, implementing, and assessing security controls; and (iv) formally authorizing the information system for operation (also known as security accreditation). The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, executive orders, policies, standards, or regulations. The following activities related to managing organizational risk 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—

- ***Categorize*** the information system and the information resident within that system based on a FIPS 199 impact analysis.
- ***Select*** an initial set of security controls (i.e., baseline) for the information system as a starting point based on the FIPS 199 security categorization.
- ***Adjust*** (or tailor) the initial set of security controls based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses, the availability of compensating controls, or special circumstances.
- ***Document*** the agreed-upon set of security controls in the system security plan including the organization's justification for any refinements or adjustments to the initial set of controls.
- ***Implement*** the security controls in the information system. For legacy systems, some or all of the security controls selected may already be in place.
- ***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.
- ***Determine*** the risk to organizational operations and assets resulting from the planned or continued operation of the information system.

Draft

- ***Authorize*** information system processing (or for legacy systems, authorize continued system processing) if the level of risk to the organization's operations or assets is acceptable.[14]
- ***Monitor*** 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.

The remainder of this chapter focuses on the first two activities in managing organizational risk—security categorization and the initial selection and specification of security controls based on the FIPS 199 security categorization.

3.2 SECURITY CATEGORIZATION AND BASELINE SELECTION

FIPS 199, the mandatory 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 system's criticality and sensitivity. FIPS 199 assigns this level of criticality and sensitivity based on the potential impact on organizational operations, organizational assets, or individuals should there be a breach in security due to the loss of confidentiality, integrity, or availability. FIPS 199 requires organizations to categorize their information systems as low, moderate, 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.[15] The generalized format for expressing the security category, SC, of an information system is:

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

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.[16] 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. Once the overall impact

[14] 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.

[15] 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.

[16] 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 adjustments to or tailoring of the security control baselines (see Section 3.3).

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.

3.3 TAILORING THE INITIAL BASELINE

After the appropriate security control baseline is selected, there are two additional steps needed to tailor the baseline for a specific organizational information system: (i) the application of *scoping guidance* to the initial baseline; and (ii) the specification of *organization-defined parameters* in the security controls, where appropriate.

Scoping Guidance

Scoping guidance provides organizations with specific considerations on the applicability and implementation of individual security controls in the control baseline. There are four types of considerations that can potentially impact how the baseline controls are applied: (i) technology-related considerations; (ii) infrastructure-related considerations; (iii) common security control-related considerations; and (iv) risk-related considerations.

Technology-related considerations—

- Security controls that refer to specific technologies (e.g., wireless, cryptography) are only applicable if those technologies are employed or are required to be employed within the information system.
- Security controls are only applicable to the components of the information system that typically provide the security capability addressed by the control. For information system components that are single-user, not networked, or only locally networked, one or more of these characteristics provide appropriate rationale for not applying selected controls to that component.
- Security controls that explicitly or implicitly refer to automated mechanisms do not require the development of such mechanisms, but instead require the use of existing mechanisms to the extent that the mechanisms are readily available in commercial or government off-the-shelf products. In situations where automated mechanisms are not readily available or technically feasible, manual mechanisms or procedures can be employed to satisfy security control requirements.

Infrastructure-related considerations—

- Security controls that refer to organizational facilities are only applicable to those sections of the facilities where there are concentrations of information technology assets (i.e., electronic mail or web servers, server farms, data centers, networking nodes, controlled interface equipment, and communications equipment, but not to those sections containing only workstations or related peripherals).
- Security controls that refer to environmental matters (e.g., temperature, humidity, lighting, and power) are generally only applicable to organizational facilities as described above.

Common security control-related considerations—

- Security controls designated by the organization as common controls are 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. Decisions on common control designations will not, however, affect the organization's responsibility in providing the security controls included in the baseline.

Draft

Risk-related considerations—

- Security controls that largely support the availability security objective 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 is consistent with the FIPS 199 security categorization prior to moving to the high water mark and is supported by an organizational assessment of risk. The security controls in the Contingency Planning (CP) family and the environment-related controls from the Physical and Environmental Protection (PE) family (i.e., PE-9 through PE-20) are candidates for downgrading actions. Organizations have some latitude in downgrading other availability-related security controls as long as the controls do not support the security objectives of confidentiality and/or integrity.

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. After the application of the scoping guidance, organizations should review the list of security controls for assignment and selection operations and provide 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, directives, executive orders, policies, standards, or regulations or are indicated by the risk assessment in order to adequately mitigate risk.

3.4 SUPPLEMENTING THE INITIAL BASELINE

The security control baselines listed in Appendix D should be viewed as foundations or starting points in the selection of adequate security controls for information systems. The baselines represent, for classes of information systems (derived from FIPS 199 security categorizations), the minimum level of *due diligence* 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 is a function of the organization's assessment of risk. In many cases, additional or enhanced security controls will be needed to address specific threats to and vulnerabilities in the information system or to satisfy the requirements of applicable laws, directives, executive orders, policies, standards, or regulations. 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 current baselines. The techniques and methodologies used by organizations in supplementing the security control baselines are beyond the scope of this special publication.

APPENDIX A

REFERENCES

LAWS, DIRECTIVES, POLICIES, STANDARDS, AND GUIDELINES

1. Committee for National Security Systems Instruction 4009, *National Information Assurance Glossary*, May 2003.
2. Department of Defense Instruction 8500.2, *Information Assurance Implementation*, February 2003.
3. Department of Health and Human Services Centers for Medicare and Medicaid Services, *Core Security Requirements*, February 2004.
4. Director of Central Intelligence Directive Manual 6/3, *Protecting Sensitive Compartmented Information within Information Systems*, May 2000.
5. Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems*, December 2003.
6. Federal Information Processing Standards 200, *Security Controls for Federal Information Systems* (projected for publication December 2005).
7. Federal Information Security Management Act (Public Law 107-347), December 2002.
8. General Accounting Office *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6, January 1999.
9. Information Technology Management Reform Act (Public Law 104-106), August 1996.
10. International Organization for Standardization/International Electrotechnical Commission 17799:2000, *Code of Practice for Information Security Management*, December 2000.
11. National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.
12. National Institute of Standards and Technology Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.
13. 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.
14. National Institute of Standards and Technology Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.
15. National Institute of Standards and Technology Special Publication 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, Revision A, June 2004.
16. National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.
17. National Institute of Standards and Technology Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.
18. National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services*, October 2003.

Draft

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

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

21. National Institute of Standards and Technology Special Publication 800-40, *Procedures for Handling Security Patches*, September 2002.

22. National Institute of Standards and Technology Special Publication 800-45, *Guidelines on Electronic Mail Security*, September 2002.

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

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

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

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

27. National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (projected for publication winter 2004-05).

28. National Institute of Standards and Technology Special Publication 800-56, *Recommendation on Key Establishment Schemes*, (initial public draft) January 2004.

29. National Institute of Standards and Technology Special Publication 800-57, *Recommendation on Key Management*, (initial public draft) January 2004.

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

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

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

33. National Institute of Standards and Technology Special Publication 800-63, *Electronic Authentication Guideline*, June 2004.

34. National Institute of Standards and Technology Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle*, October 2003.

35. National Institute of Standards and Technology Special Publication 800-65, *Integrating Security into the Capital Planning and Investment Control Process* (initial public draft), July 2004.

36. National Institute of Standards and Technology Special Publication 800-70, *The NIST Security Configuration Checklists Program* (initial public draft), August 2004.

37. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

Draft

38. Office of Management and Budget, Federal Enterprise Architecture Program Management Office, *Business Reference Model* (v2.0), June 2003.
39. Paperwork Reduction Act of 1995 (Public Law 104-13), May 1995.
40. Privacy Act of 1974 (Public Law 93-579), September 1975.

Draft

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

Accreditation	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.
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.
Assessment Method	A focused activity or action employed by an assessor for evaluating a particular attribute of a security control.
Assessment Procedure	A set of activities or actions employed by an assessor to determine the extent to which a security control is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the 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.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authorize Processing	See Accreditation.
Authorizing Official	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.
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
Certification Agent	The individual, group, or organization responsible for conducting a security certification.

Draft

Certification	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.
Chief Information Officer [44 U.S.C., 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.
Common Security Control	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.
Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
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.
Configuration Control [CNSS Inst. 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.
Controlled Interface [CNSS Inst. 4009]	Mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected 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.

Draft

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.
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 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 responsible to the senior agency information security officer, authorizing official, or information system owner for ensuring the appropriate operational security posture is maintained 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.

Draft

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.
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.
Major Information System [FISMA]	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.
Management Controls [NIST SP 800-18]	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.
Minor Application	An application, other than a major application, that requires 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. Minor applications are typically included as part of a general support system.
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.

Draft

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 [NIST SP 800-18]	The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).
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]	Low: The loss of confidentiality, integrity, or availability could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals. Moderate: The loss of confidentiality, integrity, or availability could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals. High: The loss of confidentiality, integrity, or availability could be expected to have a *severe* or *catastrophic* adverse effect 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.
Risk [NIST SP 800-30]	The level of impact on agency operations (including mission, functions, image, or reputation), agency 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]	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
Risk Management [NIST SP 800-30]	The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.

Draft

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.
Sanitization [CNSS Inst. 4009, Adapted]	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.
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 Impact Analysis	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 Objective	Confidentiality, integrity, or availability.
Security Plan	See System Security Plan.
Security Requirements [CNSS Inst. 4009, Adapted]	Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet laws, executive orders, directives, policies, or regulations.
Senior Agency Information Security Officer	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.
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	A security control for an information system that has not been designated as a common security control.
System Security Plan [NIST SP 800-18]	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.

Draft

Technical Controls [NIST SP 800-18, Adapted]	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 Agent/Source [NIST SP 800-30]	Either: (i) intent and method targeted at the intentional exploitation of a vulnerability; or (ii) a situation and method that may accidentally trigger a vulnerability.
Threat Assessment [CNSS Inst. 4009]	Formal description and evaluation of threat to 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.

Draft

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

CIO	Chief Information Officer
CNSS	Committee for National Security Systems
COTS	Commercial Off The Shelf
DCID	Director of Central Intelligence Directive
FIPS	Federal Information Processing Standard(s)
FISMA	Federal Information Security Management Act
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
USC	United States Code

Draft

APPENDIX D

MINIMUM SECURITY CONTROLS

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. An "X" marked in one of the three baselines indicates the selection of a particular security control for that baseline. Control enhancements, when used to supplement basic security controls, are indicated by the number of the control enhancement. For example, an "X (1) (2)" 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 enhancements (1) and (2). Some security controls in the security control catalog are not used in any of the baselines but are available for optional use by organizations when indicated based on the results of a risk assessment. The compete description of the security controls, supplemental guidance for the controls, and control enhancements is provided in Appendix F.

Draft

CONTROL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
Access Control				
AC-1	Access Control Policy and Procedures	X	X	X
AC-2	Account Management	X	X (1) (2) (3)	X (1) (2) (3) (4)
AC-3	Access and Information Flow Control	X	X (1)	X (1)
AC-4	Separation of Duties	X	X	X
AC-5	Least Privilege	---	X	X
AC-6	Unsuccessful Logon Attempts	X	X	X
AC-7	System Use Notification	X	X	X
AC-8	Privacy Policy Notification	X	X	X
AC-9	Previous Logon Notification	---	X	X
AC-10	Concurrent Session Control	---	---	X
AC-11	Session Lock	---	X	X
AC-12	Session Termination	---	X	X
AC-13	Supervision and Review—Access Control	X	X (1)	X (1)
AC-14	Permitted Actions w/o Identification or Authentication	X	X (1)	X (1)
AC-15	Automated Marking	---	---	X
AC-16	Automated Labeling	---	---	---
AC-17	Remote Access	X	X (1) (2) (3)	X (1) (2) (3)
AC-18	Wireless Access Restrictions	X	X (1)	X (1)
Awareness and Training				
AT-1	Security Awareness and Training Policy and Procedures	X	X	X
AT-2	Security Awareness	X	X	X
AT-3	Security Training	X	X	X
AT-4	Security Training Records	X	X	X
Audit and Accountability				
AU-1	Audit and Accountability Policy and Procedures	X	X	X
AU-2	Auditable Events	X	X (1)	X (1)
AU-3	Content of Audit Records	X	X (1)	X (1) (2)
AU-4	Audit Storage Capacity	X	X	X
AU-5	Audit Processing	X	X	X (1)
AU-6	Audit Monitoring, Analysis, and Reporting	X	X (1)	X (1) (2)
AU-7	Audit Reduction and Report Generation	---	X	X (1)
AU-8	Time Stamps	---	X	X
AU-9	Protection of Audit Information	X	X	X
AU-10	Non-repudiation	---	---	---
Certification, Accreditation, and Security Assessments				
CA-1	Certification, Accreditation, and Security Assessment Policy and Procedures	X	X	X
CA-2	Security Assessment	X	X	X
CA-3	Information System Connections	X	X	X

Draft

CONTROL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-4	Security Certification	X	X	X
CA-5	Plan of Action and Milestones	X	X	X
CA-6	Security Accreditation	X	X	X
CA-7	Continuous Monitoring	X	X	X
Configuration Management				
CM-1	Configuration Management Policy and Procedures	X	X	X
CM-2	Baseline Configuration	X	X (1) (2)	X (1) (2)
CM-3	Configuration Change Control	X	X (1)	X (1)
CM-4	Monitoring Configuration Changes	X	X	X
CM-5	Access Restrictions for Change	X	X (1)	X (1)
CM-6	Configuration Settings	X	X	X (1)
Contingency Planning				
CP-1	Contingency Planning Policy and Procedures	X	X	X
CP-2	Contingency Plan	X	X (1)	X (1)
CP-3	Contingency Training	---	X	X (1) (2)
CP-4	Contingency Plan Testing	---	X	X (1) (2) (3)
CP-5	Contingency Plan Update	X	X	X
CP-6	Alternate Storage Sites	---	X (1)	X (1) (2) (3)
CP-7	Alternate Processing Sites	---	X (1) (2) (3)	X (1) (2) (3) (4)
CP-8	Alternate Telecommunications Services	---	X (1) (2)	X (1) (2) (3) (4)
CP-9	Information System Backup	X	X (1)	X (1) (2) (3)
CP-10	Information System Recovery and Reconstitution	X	X	X (1)
Identification and Authentication				
IA-1	Identification and Authentication Policy and Procedures	X	X	X
IA-2	User Identification and Authentication	X	X	X
IA-3	Device Authentication and Authentication	X	X	X
IA-4	Identifier Management	X	X	X
IA-5	Authenticator Management	X	X	X
IA-6	Authenticator Feedback	X	X	X
IA-7	Cryptographic Module Authentication	X	X	X
Incident Response				
IR-1	Incident Response Policy and Procedures	X	X	X
IR-2	Incident Response Training	---	X (1)	X (1) (2)
IR-3	Incident Response Testing	---	X (1)	X (1)
IR-4	Incident Handling	X	X (1)	X (1)
IR-5	Incident Monitoring	---	X	X (1)
IR-6	Incident Reporting	X	X (1)	X (1)
IR-7	Incident Response Assistance	X	X (1)	X (1)
Maintenance				
MA-1	System Maintenance Policy and Procedures	X	X	X

CONTROL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-2	Periodic Maintenance	X	X (1)	X (1)
MA-3	Maintenance Tools	---	X	X (1) (2) (3)
MA-4	Remote Maintenance	X	X	X (1) (2)
MA-5	Maintenance Personnel	---	X	X
MA-6	Timely Maintenance	---	X	X
Media Protection				
MP-1	Media Protection Policy and Procedures	X	X	X
MP-2	Media Access	X	X	X (1)
MP-3	Media Labeling	---	X	X
MP-4	Media Storage	---	X	X
MP-5	Media Transport	---	---	X
MP-6	Media Sanitization	---	X	X
MP-7	Media Destruction and Disposal	---	X	X
MP-8	Media-related Records	---	---	X
Physical and Environmental Protection				
PE-1	Physical and Environmental Protection	X	X	X
PE-2	Physical Access Authorizations	X	X	X
PE-3	Physical Access Control	X	X	X
PE-4	Access Control for Transmission Medium	---	---	X
PE-5	Access Control for Display Medium	---	X	X
PE-6	Monitoring Physical Access	X	X (1)	X (1) (2)
PE-7	Visitor Control	X	X (1)	X (1)
PE-8	Access Logs	X	X (1)	X (1)
PE-9	Power Equipment and Cabling	---	X	X
PE-10	Emergency Shutoff	X	X	X
PE-11	Emergency Power	X	X (1)	X (1) (2) (3)
PE-12	Emergency Lighting	X	X	X
PE-13	Fire Protection	X	X (1)	X (1) (2)
PE-14	Temperature and Humidity Controls	X	X	X
PE-15	Water Damage Protection	X	X	X (1)
PE-16	Environmental Controls Training	---	---	X
PE-17	Environmental Controls Testing	---	---	X
PE-18	Delivery and Removal	X	X	X
PE-19	Alternate Work Site	---	X	X
PE-20	Access Control for Portable and Mobile Systems	X	X (1)	X (1)
Planning				
PL-1	Security Planning Policy and Procedures	X	X	X
PL-2	System Security Plan	X	X	X
PL-3	System Security Plan Update	X	X	X
PL-4	Rules of Behavior	X	X	X

CONTROL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
PL-5	Privacy Impact Assessment	X	X	X
Personnel Security				
PS-1	Personnel Security Policy and Procedures	X	X	X
PS-2	Position Categorization	X	X	X
PS-3	Personnel Screening	X	X	X
PS-4	Personnel Termination	X	X	X
PS-5	Personnel Transfer	X	X	X
PS-6	Access Agreements	X	X	X
PS-7	Third-Party Personnel Security	X	X	X
PS-8	Personnel Sanctions	X	X	X
Risk Assessment				
RA-1	Risk Assessment Policy and Procedures	X	X	X
RA-2	Security Categorization	X	X	X
RA-3	Risk Assessment	X	X	X
RA-4	Risk Assessment Update	X	X	X
System and Services Acquisition				
SA-1	System and Services Acquisition Policy and Procedures	X	X	X
SA-2	Allocation of Resources	X	X	X
SA-3	Life Cycle Support	X	X	X
SA-4	Acquisitions	X	X	X
SA-5	Information System Documentation	X	X	X
SA-6	Software Usage Restrictions	X	X	X
SA-7	User Installed Software	X	X	X (1)
SA-8	Security Design Principles	---	X	X
SA-9	Outsourced Information System Services	X	X	X
System and Communications Protection				
SC-1	System and Communications Policy and Procedures	X	X	X
SC-2	Application Partitioning	---	X	X
SC-3	Security Function Isolation	---	X	X (1)
SC-4	Information Remnants	---	X	X
SC-5	Denial of Service Protection	X	X	X
SC-6	Resource Priority	---	X	X
SC-7	Boundary Protection	X	X (1)	X (1)
SC-8	Transmission Integrity	---	X	X
SC-9	Transmission Confidentiality	---	X	X
SC-10	Network Disconnect	---	X	X
SC-11	Trusted Path	---	---	X
SC-12	Cryptographic Key Establishment and Management	---	X	X
SC-13	Cryptographic Operations	---	X	X
SC-14	Public Access Protections	X	X	X

CONTROL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-15	Collaborative Computing	---	---	X
SC-16	Transmission of Security Parameters	---	---	---
SC-17	Public Key Infrastructure Certificates	---	---	X
SC-18	Mobile Code	---	X	X
System and Information Integrity				
SI-1	System and Information Integrity Policy and Procedures	X	X	X
SI-2	Flaw Remediation	X	X	X
SI-3	Malicious Code Protection	X	X	X (1)
SI-4	Intrusion Detection Tools and Techniques	---	X	X
SI-5	Security Alerts and Advisories	---	X	X
SI-6	Security Functionality Verification	---	X	X (1)
SI-7	Software and Information Integrity	---	---	X

Draft

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 of security control developers and implementers and are applied on a control-by-control basis. For ease of use, the assurance requirements are grouped by baselines. 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. During the assessment of the security controls (described in NIST Special Publication 800-53A), assessors will be attempting 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 information system. Complying with the minimum assurance requirements is necessary in order to gain confidence in the overall effectiveness of the security controls employed within the information system.

Low Baseline

Requirement: **The security control is in effect and meets explicitly identified requirements.**

Supplemental Guidance: For security controls in the low baseline, the focus 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.

Moderate Baseline

Requirement: The security control is in effect and meets explicitly identified requirements. **The control developer/implementer includes, as an integral part of the control, actions to ensure that, when the control is implemented, it will meet its required function or purpose. These actions include 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 ensuring control correctness. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer/implementer incorporates, as part of the control, specific capabilities to ensure the control meets its function or purpose. The following examples are illustrative:

- For controls primarily resulting in a specification (e.g., a contingency plan, an incident response plan, configuration change control procedure), the specification explicitly assigns responsibilities and identifies actions to be taken, as an integral part of the associated control implementation, to ensure that the control is being applied and followed.
- For controls consisting primarily of people-oriented activities (e.g., establishing information system accounts, controlling physical access points), the control includes, as an integral part of the activity, actions to ensure that the activity is being conducted.
- For controls implemented primarily by hardware, software and/or firmware (e.g., intrusion detection software, user identification and authentication mechanisms), the control developer/implementer defines, as an integral part of the control, the steps necessary to fully verify the required functionality of the control.

Draft

High Baseline

Requirement: The security control is in effect and meets explicitly identified requirements. The control developer/implementer includes, as an integral part of the control, actions to ensure that, when the control is implemented, it will **continuously and consistently (i.e., across the information system)** meet its required function or purpose. These actions include requiring the development of records with structure and content suitable to facilitate making this determination. **The control developer/implementer also includes, as an integral part of the control, actions to support improvement in the effectiveness of the control. These actions include requiring the development of records with structure and content suitable for facilitating/enabling improvement in the control's effectiveness.**

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 to support continuous improvement in the control's effectiveness. The following examples are illustrative:

- For controls primarily resulting in a specification (e.g., a contingency plan, an incident response plan, configuration change control procedure), the specification explicitly assigns responsibilities and identifies actions to be taken, as an integral part of the associated control implementation, to ensure that the control is being applied and followed. This includes ensuring consistent application across the system on an ongoing basis.
- For controls consisting primarily of people-oriented activities (e.g., establishing information system accounts, controlling physical access points), the control includes, as an integral part of the activity, actions to ensure that the activity is being conducted and to support improvement in the effectiveness of the activity.
- For controls implemented primarily by hardware, software and/or firmware (e.g., intrusion detection software, user identification and authentication mechanisms), the control developer/implementer defines, as an integral part of the control, the steps necessary to fully verify the required functionality of the control. The control also includes a self-checking capability to ensure that the control continues to operate as intended. This capability can be: (i) automated; (ii) manual actions incorporated into the procedures implemented as a part of the control; or (iii) a combination of the two.

Additional Requirements Supplementing the High Baseline

Requirement: The security control is in effect and meets explicitly identified requirements. The control developer/implementer includes, as an integral part of the control, actions to ensure that, when the control is implemented, it will continuously and consistently (i.e., across the information system) meet its required function or purpose. These actions include requiring the development of records with structure and content suitable for making this determination. The control developer/implementer also includes, as an integral part of the control, actions to support improvement in the effectiveness of the control. These actions include requiring the development of records with structure and content suitable for facilitating/enabling improvement in the control's effectiveness. **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 high baseline, when appropriate, in order to protect against threats from highly skilled, highly motivated, and well-financed threat agents. This level of protection is required for those information systems where the organization is not willing to accept the risks associated with the type of threat agents cited above. The following examples are illustrative:

- For controls primarily resulting in a specification (e.g., a contingency plan, an incident response plan, configuration change control procedure), the specification explicitly assigns responsibilities and identifies actions to be taken, as an integral part of the associated control implementation, to ensure that the control is being applied and followed. This includes ensuring consistent application across the system on an ongoing basis. In addition, an analysis is performed that supports a high degree of confidence that the specification is complete, consistent, and correct.

- For controls consisting primarily of people-oriented activities (e.g., establishing information system accounts, controlling physical access points), the control includes, as an integral part of the activity, actions to ensure that the activity is being conducted and to support analysis of and improvement in the effectiveness of the activity.
- For controls implemented primarily by hardware, software and/or firmware (e.g., intrusion detection software, user identification and authentication mechanisms), the control developer/implementer defines, as an integral part of the control, the steps necessary to fully verify the required functionality of the control. The control also includes a self-checking capability to ensure that the control continues to operate as intended. This capability can be: (i) automated; (ii) manual actions incorporated into the procedures implemented as a part of the control; or (iii) a combination of the two. In addition, the control should be implemented on the basis of and in conjunction with an analysis that clearly and unambiguously supports a high degree of confidence that the control is implemented correctly, is always invoked, cannot be bypassed, and is protected from tampering and corruption.

Draft

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 function 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 with 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 main body of the control.

The supplemental guidance section provides additional information related to a specific security control. Supplemental guidance should be considered by organizations when defining, developing, and implementing security controls. Applicable federal legislation, 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 additional statements of security capability needed to strengthen a basic control when the control is used in an information system requiring greater protection due to the potential impact of loss or when organizations seek additional control strength 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.

With regard to cryptography employed in federal information systems, organizations must comply with current federal policy and meet the requirements of FIPS 140-2, *Security Requirements for Cryptographic Modules*. The FIPS 140-2 standard also acknowledges the use of cryptography approved by the National Security Agency as an appropriate alternative for organizations. Consult FIPS 140-2 for specific guidance.

Draft

FAMILY: ACCESS CONTROL (AC)

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, 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 federal laws, 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.

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 time period*].

Supplemental Guidance: Account management includes the identification of account types (i.e., individual, group, 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 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. The organization ensures that account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured.

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 ensure that account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals are notified.

Draft

AC-3 ACCESS AND INFORMATION FLOW CONTROL

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

Supplemental Guidance:

Access control
Access control policies and enforcement mechanisms are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, fields, processes, programs, domains) in the information system. Access control policies and associated enforcement mechanisms can be *role-based* or *identity-based*. Where encryption of stored information is used as an access enforcement mechanism, the cryptography used is FIPS 197 or FIPS 46-3 (Triple DES) compliant and implemented using FIPS 140-2 validated cryptographic modules.

Information flow control
Information flow control policies and enforcement mechanisms are employed by organizations to control the flow of information between designated sources and destinations (e.g., individuals, devices) within the information system based on the characteristics of the information. Simple examples of flow control enforcement can be found in firewall and router devices that employ rule sets or establish configuration settings that limit or restrict information system services or provide a packet filtering capability. More sophisticated (and less common) examples of flow control enforcement can be found in information systems that use explicit labels on information, source, and destination objects as the basis for flow control decisions. For example, some organizations may require flow control policies for controlling the release of certain types of information.

Enforcement mechanisms
Enforcement mechanisms within an information system (e.g., access control lists, cryptography) that support access control and information flow control can be discretionary or mandatory (i.e., non-discretionary). Discretionary enforcement mechanisms allow users to specify and control sharing of objects by users, or by defined groups of users, or by both. Mandatory enforcement mechanisms implement organization-defined authorizations allowing only authorized users to specify and control sharing of objects by users, or by defined groups of users, or by both. Where a mandatory access control policy is defined, it is enforced over all users (or processes acting on behalf of users) and objects covered by the policy (e.g., devices, files, records, fields, processes, programs, domain).

Control Enhancements:

(1) The information system ensures that access to security critical functions (deployed in hardware, software, and firmware) and information is restricted to authorized personnel (e.g., system security administrators).

AC-4 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.

AC-5 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.

AC-6 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 until released by an administrator, 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: None.

Control Enhancements: None.

AC-7 SYSTEM USE NOTIFICATION

Control: The information system displays an approved, standardized notification message prior to 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 notification message provides appropriate privacy and security notices and remains on the screen until the user takes explicit actions to log on to the information system.

Supplemental Guidance: For publicly accessible systems: (i) the system use information is available as opposed to displaying the information prior to granting access; (ii) there are no references to monitoring, recording, or auditing since privacy accommodations for such systems 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.

AC-8 PRIVACY POLICY NOTIFICATION

Control: The information system displays the organization's privacy policy prior to granting system access.

Supplemental Guidance: The privacy policy is consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.

Control Enhancements: None.

AC-9 PREVIOUS LOGON NOTIFICATION

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

Supplemental Guidance: None.

Control Enhancements: None.

Draft

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.

AC-11 SESSION LOCK

Control: The information system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

Supplemental Guidance: Users can directly initiate session lock mechanisms. The information system also activates session lock mechanisms automatically after a specified period of inactivity defined by the organization. A session lock is not a substitute for logging out of the information system.

Control Enhancements: None.

AC-12 SESSION TERMINATION

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

Supplemental Guidance: None.

Control Enhancements: None.

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.

Control Enhancements:

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

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control: The organization identifies 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.

Control Enhancements:

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

Draft

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: None.

Control Enhancements: None.

AC-16 AUTOMATED LABELING

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

Supplemental Guidance: Information labeling is accomplished in accordance with special dissemination, handling, or distribution instructions, or as otherwise required to enforce information system security policy.

Control Enhancements: None.

AC-17 REMOTE ACCESS

Control: The organization documents, monitors, and controls all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.

Supplemental Guidance: 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). The organization permits remote access for privileged functions only for compelling operational needs.

Control Enhancements:

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

(2) The organization uses encryption to protect the confidentiality of remote access sessions.

(3) The organization controls all remote accesses through a managed access control point.

AC-18 WIRELESS ACCESS RESTRICTIONS

Control: The organization documents, monitors, and controls wireless access to the information system.

Supplemental Guidance: NIST Special Publication 800-48 provides guidance on wireless network security.

Control Enhancements:

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

Draft

FAMILY: SECURITY AWARENESS AND TRAINING (AT)

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, 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 federal laws, 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 Publication 800-50 provides guidance on security awareness and training. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

AT-2 SECURITY AWARENESS

Control: The organization trains all personnel (including managers and senior executives) in basic information system security awareness prior to authorizing access to the system and [*Assignment: organization-defined time period, 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.

Control Enhancements: None.

AT-3 SECURITY TRAINING

Control: The organization identifies personnel with significant information system security roles and responsibilities, documents those roles and responsibilities, and provides appropriate information system security training prior to authorizing access to the system and [*Assignment: organization-defined time period*] 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.

Control Enhancements: None.

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.

Draft

FAMILY: AUDIT AND ACOUNTABIITY (AU)

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, 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 federal laws, 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.

AU-2 AUDITABLE EVENTS

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

Supplemental Guidance: 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. 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.

Control Enhancements:

(1) The organization retains audit logs for one year.

(2) 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.

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

AU-3 CONTENT OF AUDIT RECORDS

Control: The information system captures sufficient information in audit records 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) information system location of the event; (iii) type of event; (iv) subject identity; and (v) the outcome (success or failure) of the event.

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.

Draft

AU-4 AUDIT STORAGE CAPACITY

Control: The organization allocates sufficient audit record storage capacity to reduce the potential for such capacity being exceeded.

Supplemental Guidance: None.

Control Enhancements: None.

AU-5 AUDIT PROCESSING

Control: In the event of an audit failure or audit storage capacity is reached, the information system alerts appropriate organizational officials and takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shutdown information system, overwrite oldest audit records, stop generating audit records)*].

Supplemental Guidance: None.

Control Enhancements: None.

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

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

Supplemental Guidance: None.

Control Enhancements:

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

(2) The organization employs automated mechanisms to immediately alert security personnel of any inappropriate or unusual activities with security implications.

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.

AU-8 TIME STAMPS

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

Supplemental Guidance: Time stamps of audit records are generated using internal information system clocks that are synchronized systemwide.

Control Enhancements: None.

Draft

AU-9 PROTECTION OF AUDIT INFORMATION

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

Supplemental Guidance: None.

Control Enhancements:

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

AU-10 NON-REPUDIATION

Control: The information system provides the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message).

Supplemental Guidance: 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 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 digital signatures, digital message receipts, and time stamps.

Control Enhancements: None.

Draft

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS (CA)

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, 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 federal laws, 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. NIST Special Publication 800-53A provides guidance on security control assessments. NIST Special Publication 800-37 provides guidance on processing security certification and accreditation. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

CA-2 SECURITY ASSESSMENT

Control: In support of the continuous monitoring process, the organization conducts an assessment of the security controls in the information system [*Assignment: organization-defined time period, 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: The organization conducts periodic security assessments in support of the FISMA requirement to determine the effectiveness of the security controls employed within the information system and in support of a continuous monitoring process. NIST Special Publication 800-53A provides guidance on security control assessments. NIST Special Publication 800-37 provides guidance on the continuous monitoring process.

Control Enhancements: None.

CA-3 INFORMATION SYSTEM CONNECTIONS

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

Supplemental Guidance: Appropriate organizational officials approve information system interconnection agreements. NIST Special Publication 800-47 provides guidance on interconnecting information systems.

Control Enhancements: None.

Draft

CA-4 SECURITY CERTIFICATION

Control: In support of the security accreditation process, 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 requirement for accrediting the information system. The security certification is integrated into and spans the System Development Life Cycle (SDLC). NIST Special Publication 800-53A provides guidance on the assessment of security controls. NIST Special Publication 800-37 provides guidance on security certification and accreditation.

Control Enhancements: None.

CA-5 PLAN OF ACTION AND MILESTONES

Control: The organization develops and updates [*Assignment: organization-defined time period*], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct any 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 updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. The plan of action and milestones is a key document in the security accreditation package developed for the authorizing official. 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.

CA-6 SECURITY ACCREDITATION

Control: The organization authorizes (i.e., accredits) the information system for processing prior to operations and updates the authorization [*Assignment: organization-defined time period*]. 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 information systems. The organization assesses the security controls employed within the information system prior to and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications. NIST Special Publication 800-37 provides guidance on the security certification and accreditation of information systems.

Control Enhancements: None.

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 establishes the selection criteria for control monitoring and subsequently selects a subset of the security controls employed within the information system for purposes of continuous monitoring. NIST Special Publication 800-53A provides guidance on the assessment of security controls.

Control Enhancements: None.

Draft

FAMILY: CONFIGURATION MANAGEMENT (CM)

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, 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 federal laws, 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.

CM-2 BASELINE CONFIGURATION

Control: The organization develops, documents, and maintains a current, baseline configuration of the information system and an inventory of the system's constituent components.

Supplemental Guidance: The configuration of the information system is consistent with the Federal Enterprise Architecture and the organization's information system architecture. The inventory of information system components includes manufacturer, type, serial number, version number, and location (i.e., physical location and logical position within the information system architecture).

Control Enhancements:

(1) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration.

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

CM-3 CONFIGURATION CHANGE CONTROL

Control: The organization documents and controls changes to the information system. Appropriate organizational officials approve information system changes in accordance with organizational policies and procedures.

Supplemental Guidance: Configuration change control involves the systematic proposal, justification, test/evaluation, review, and disposition of proposed changes. The organization includes emergency changes in the configuration change control process.

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.

Draft

CM-4 MONITORING CONFIGURATION CHANGES

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

Supplemental Guidance: The organization documents the installation of information system components. The organization audits system programmer activities, including the use of information system utilities.

Control Enhancements: None.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control: The organization enforces access restrictions associated with changes to the information system.

Supplemental Guidance: The organization restricts access to system-level software to a limited number of personnel, corresponding to job responsibilities.

Control Enhancements:

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

CM-6 CONFIGURATION SETTINGS

Control: The organization configures the default security settings of information technology products to the most restrictive mode consistent with information system operational requirements. The organization configures the information system to provide only essential capabilities and specifically prohibits the use of the following ports, protocols, and/or services: [*Assignment: organization-defined list of ports, protocols, and/or services*].

Supplemental Guidance: The organization periodically reviews the information system to identify and eliminate unnecessary ports, protocols, and/or services (e.g., File Transfer Protocol, Hyper Text Transfer Protocol, mainframe supervisor calls). NIST Special Publication 800-70 provides guidance on configuration settings (i.e., checklists) for information technology products.

Control Enhancements:

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

Draft

FAMILY: CONTINGENCY PLANNING (CP)

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, 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 federal laws, 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.

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 multiple 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 (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).

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 time period, 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.

Draft

CP-4 CONTINGENCY PLAN TESTING

Control: The organization tests the contingency plan for the information system [*Assignment: organization-defined time period, at least annually*] using [*Assignment: organization-defined tests and exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan. Appropriate officials within the organization review the contingency plan test results and initiate corrective actions.

Supplemental Guidance: There are several methods for testing contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, functional/tabletop exercises).

Control Enhancements:

(1) The organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).

(2) The organization tests 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 periodically tests the readiness of the alternate processing site to ensure the site can actually be used when needed.

(4) The organization employs automated mechanisms to more thoroughly and effectively test the contingency plan.

CP-5 CONTINGENCY PLAN UPDATE

Control: The organization reviews the contingency plan for the information system [*Assignment: organization-defined time period, 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).

Control Enhancements: None.

CP-6 ALTERNATE STORAGE SITES

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

Supplemental Guidance: None.

Control Enhancements:

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

(2) The alternate storage site is sufficiently close to the alternate processing 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.

Draft

CP-7 ALTERNATE PROCESSING SITES

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.

Control Enhancements:

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

(4) The alternate processing site is fully configured to support a minimum required operational capability and ready to use as the operational site.

CP-8 ALTERNATE TELECOMMUNICATIONS SERVICES

Control: The organization identifies 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: None.

Control Enhancements:

(1) Alternate telecommunications service agreements contain priority of service provisions in accordance with the organization's availability requirements.

(2) Alternate telecommunications services do not share a single point of failure with primary telecommunications services.

(3) Alternate telecommunications service providers are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.

(4) Alternate telecommunications service providers have adequate contingency plans.

CP-9 INFORMATION SYSTEM BACKUP

Control: The organization conducts [*Assignment: organization-defined time period*] backups of user-level and system-level information (including system state information) contained in the information system and stores backup information at an appropriately secured 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.

Control Enhancements:

(1) The organization tests backup information [*Assignment: organization-defined time period*] to ensure 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 fire-rated container that is not collocated with the operational software.

Draft

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 the system's original state after a disruption or failure.

Supplemental Guidance: Secure information system recovery and reconstitution to the system's original state means that all system parameters (either default or organization-established) are reset, patches are reinstalled, configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled, information from the most recent backups is available, 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.

Draft

FAMILY: IDENTIFICATION AND AUTHENTICATION (IA)

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, 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 applicable federal laws, 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 electronic authentication.

Control Enhancements: None.

IA-2 USER IDENTIFICATION AND AUTHENTICATION

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

Supplemental Guidance: NIST Special Publication 800-63 provides guidance on electronic authentication.

Control Enhancements: None.

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: The information system identifies and authenticates connections to specific devices.

Supplemental Guidance: Device authentication typically uses either a shared secret or digital certificate to authenticate the identity of a device or devices involved in system communications as opposed to the users for which the devices are communicating.

Control Enhancements: None.

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) ensuring that the user identifier is issued to the intended party; (v) disabling 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).

Control Enhancements: None.

Draft

IA-5 AUTHENTICATOR MANAGEMENT

Control: The organization manages information system authenticators (e.g., tokens, passwords, key cards) by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and (iii) changing default authenticators upon information system installation.

Supplemental Guidance: Users 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 automatic expiration of passwords; (iv) prohibits password reuse for a specified number of generations; and (v) enforces periodic password changes. NIST Special Publication 800-63 provides guidance on password selection and content.

Control Enhancements: None.

IA-6 AUTHENTICATOR FEEDBACK

Control: The information system provides feedback to a user during an attempted authentication that does not weaken the strength of the authentication mechanism.

Supplemental Guidance: The information system may obscure feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password).

Control Enhancements: None.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control: For authentication to a cryptographic module, the information system employs authentication methods that meet the requirements of FIPS 140-2.

Supplemental Guidance: None.

Control Enhancements: None.

Draft

FAMILY: INCIDENT RESPONSE (IR)

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, 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 federal laws, 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 800-61 provides guidance on incident handling and reporting. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

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 time period, 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.

IR-3 INCIDENT RESPONSE TESTING

Control: The organization tests the incident response capability for the information system [*Assignment: organization-defined time period, at least annually*] using [*Assignment: organization-defined tests and exercises*] to determine the plan's effectiveness and documents the results.

Supplemental Guidance: None.

Control Enhancements:

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

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: The organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly.

Control Enhancements:

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

Draft

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 analysis of incident information.

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 federal laws, directives, policies, regulations, standards, and guidance.

Control Enhancements:

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

IR-7 INCIDENT RESPONSE ASSISTANCE

Control: The organization provides an incident 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 support resources in an organization include a help desk or an assistance group.

Control Enhancements:

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

Draft

FAMILY: MAINTENANCE (MA)

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, 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 federal laws, 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.

MA-2 PERIODIC MAINTENANCE

Control: The organization schedules, performs, and documents routine preventative and regular maintenance on the components of the information system in accordance with manufacture/vendor specifications and/or organizational requirements.

Supplemental Guidance: The organization maintains a maintenance log for the information system that includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; and (iv) a description of the maintenance performed. Appropriate 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 the security features to ensure that they are still functioning properly.

Control Enhancements:

(1) The organization employs automated mechanisms to ensure that periodic maintenance is scheduled and conducted as required, and that a log of maintenance actions, both needed and completed, is up-to-date, accurate, complete, and readily available.

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: None.

Control Enhancements:

(1) The organization inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.

(2) The organization checks all media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) 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 to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized prior to 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 ensure only authorized personnel use maintenance tools.

Draft

MA-4 REMOTE MAINTENANCE

Control: The organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.

Supplemental Guidance: The organization describes the use of remote diagnostic tools in the security plan for the information system. The organization maintains maintenance logs for all remote maintenance, diagnostic, and service activities. Appropriate organization officials periodically review maintenance logs. Other techniques to consider for improving the security of remote maintenance include: (i) encryption and decryption of diagnostic communications; (ii) strong identification and authentication techniques, such as tokens; and (iii) remote disconnect verification. When remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections. If password-based authentication is used during remote maintenance, the organization changes the passwords following each remote maintenance service.

Control Enhancements:

(1) The organization performs keystroke monitoring for remote maintenance activities.

(2) The organization addresses the installation and use of remote diagnostic links in the security plan for the information system. Remote diagnostic or maintenance services are acceptable if performed by a service or organization that implements for its own information system the same level of security as that implemented on the information system being serviced. If remote diagnostic or maintenance services are required from a service or organization that does not implement for its own information system the same level of security as that implemented on the system being serviced, the system being serviced is sanitized and physically separated from other information systems prior to the connection of the remote access line. If the information system cannot be sanitized (e.g., due to a system failure), remote maintenance is not allowed.

MA-5 MAINTENANCE PERSONNEL

Control: The organization maintains a list of individuals authorized to perform maintenance on the information system. Only authorized individuals perform maintenance on the information system.

Supplemental Guidance: Maintenance personnel have appropriate access authorizations to the information system when maintenance activities allow access to organizational information. 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.

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.

FAMILY: MEDIA PROTECTION (MP)

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, 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 federal laws, 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.

MP-2 MEDIA ACCESS

Control: The organization ensures that only authorized users have access to information in printed form or on digital media removed from the information system.

Supplemental Guidance: None.

Control Enhancements:

(1) Unless guard stations control access to media storage areas, the organization employs automated mechanisms to ensure only authorized access to such storage areas and to audit access attempts and access granted.

MP-3 MEDIA LABELING

Control: The organization affixes external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information. The organization exempts the following specific types of media or hardware components from labeling so long as they remain within a secure environment: [*Assignment: organization-defined list of media types and hardware components*].

Supplemental Guidance: The organization marks human-readable output appropriately in accordance with applicable policies and procedures. At a minimum, the organization affixes printed output with cover sheets and labels digital media with the distribution limitations, handling caveats, and applicable security markings, if any, of the information.

Control Enhancements: None.

MP-4 MEDIA STORAGE

Control: The organization physically controls and securely stores information system media, both paper and electronic, based on the highest FIPS 199 security category of the information recorded on the media.

Supplemental Guidance: The organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. The organization protects unmarked media at the highest FIPS 199 security category for the information system until the media are reviewed and appropriately labeled. Physical security containers and storage facilities are compliant with General Services Administration policy, requirements, and guidance.

Control Enhancements: None.

Draft

MP-5 MEDIA TRANSPORT

Control: The organization controls information system media (paper and electronic) and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.

Supplemental Guidance: None.

Control Enhancements: None.

MP-6 MEDIA SANITIZATION

Control: The organization sanitizes information system magnetic media using approved equipment, techniques, and procedures. The organization tracks, documents, and verifies media sanitization actions and periodically tests sanitization equipment/procedures to ensure correct performance.

Supplemental Guidance: Sanitization is the process used to remove information from magnetic media such that information recovery is not possible. Sanitization includes removing all labels, markings, and activity logs. Sanitization techniques, including degaussing and overwriting memory locations, ensure that organizational information is not disclosed to unauthorized individuals when such media is reused or disposed. The National Security Agency maintains a listing of approved products with degaussing capability. The product selected is appropriate for the type of media being degaussed.

Control Enhancements: None.

MP-7 MEDIA DESTRUCTION AND DISPOSAL

Control: The organization sanitizes or destroys information system digital media prior to its disposal or release for reuse outside the organization, to prevent unauthorized individuals from gaining access to and using the information contained on the media.

Supplemental Guidance: The organization: (i) sanitizes information system hardware and machine-readable media using approved methods before being released for reuse outside of the organization; or (ii) destroys the hardware/media. The organization destroys information storage media when no longer needed in accordance with organization-approved methods and organizational policy and procedures. The organization tracks, documents, and verifies media destruction and disposal actions. The organization physically destroys nonmagnetic (optical) media (e.g., compact disks, digital video disks) in a safe and effective manner.

Control Enhancements: None.

MP-8 MEDIA-RELATED RECORDS

Control: The organization maintains inventory and disposition records for information system digital media to ensure control and accountability of organizational information.

Supplemental Guidance: The organization uses logs for receipt of information system digital media. Media logs contain: (i) the name of media recipient; (ii) signature of media recipient; (iii) date/time media received; (iv) media control number and contents; (v) movement or routing information; and (vi) if disposed of, the date, time, and method of destruction. Logs permit information system storage media containing organizational information (including those used only for backups) to be identified and controlled.

Control Enhancements: None.

Draft

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

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, 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 federal laws, 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.

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control: The organization develops and keeps current lists of personnel with authorized access to facilities containing information systems and issues appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization review and approve the access list and authorization credentials [*Assignment: organization-defined time period, at least annually*].

Supplemental Guidance: The organization promptly removes personnel no longer requiring access from access lists.

Control Enhancements: None.

PE-3 PHYSICAL ACCESS CONTROL

Control: The organization controls all physical access points (including designated entry/exit points) to facilities containing information systems and verifies individual access authorizations before granting access to the facilities. The organization also 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. After an emergency-related event, the organization restricts reentry to facilities to authorized individuals only. 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.

Control Enhancements: None.

Draft

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control: The organization controls physical access to information system transmission lines carrying unencrypted information to prevent eavesdropping, in-transit modification, disruption, or physical tampering.

Supplemental Guidance: None.

Control Enhancements: None.

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.

PE-6 MONITORING PHYSICAL ACCESS

Control: The organization monitors physical access to information systems to detect and respond to incidents.

Supplemental Guidance: The organization reviews physical access logs periodically, investigates apparent security violations or suspicious physical access activities, and takes remedial actions.

Control Enhancements:

(1) The organization centrally monitors real-time intrusion alarms and surveillance equipment.

(2) The organization employs automated mechanisms to ensure potential intrusions are recognized and appropriate response actions initiated.

PE-7 VISITOR CONTROL

Control: The organization controls physical access to information systems by authenticating visitors (including government contractors) prior to authorizing access to facilities or areas other than areas designated as publicly accessible.

Supplemental Guidance: Government contractors with permanent authorization credentials are not considered visitors.

Control Enhancements:

(1) The organization escorts visitors and monitors visitor activity, when required.

PE-8 ACCESS LOGS

Control: The organization maintains a visitor access log 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 access logs [*Assignment: organization-defined time period*] after closeout.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the maintenance and review of access logs.

Draft

PE-9 POWER EQUIPMENT AND CABLING

Control: The organization protects power equipment and cabling for the information system from damage and destruction.

Supplemental Guidance: None.

Control Enhancements: None.

PE-10 EMERGENCY SHUTOFF

Control: For specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, mainframe rooms), the organization employs and maintains a master power switch or emergency cut-off switch, prominently marked and protected by a cover to prevent accidental shutoff.

Supplemental Guidance: None.

Control Enhancements: None.

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 capable of maintaining full operational capability in the event of an extended loss of the primary power source.

(3) The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.

PE-12 EMERGENCY LIGHTING

Control: The organization employs and maintains automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes.

Supplemental Guidance: None.

Control Enhancements: None.

PE-13 FIRE PROTECTION

Control: The organization employs and maintains fire suppression and prevention devices/systems that can be activated in the event of a fire.

Supplemental Guidance: Fire suppression and prevention devices/systems include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Control Enhancements:

(1) Fire suppression and prevention devices/systems activate automatically in the event of a fire.

(2) Fire suppression and prevention devices/systems provide automatic notification of any activation to the organization and emergency responders.

Draft

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control: The organization regularly maintains within acceptable levels and monitors the temperature and humidity within facilities containing information systems.

Supplemental Guidance: None.

Control Enhancements: None.

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 ensuring that master shutoff valves are accessible, working properly, and known to key personnel.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs automated mechanisms to automatically close shutoff valves in the event of a significant water leak.

PE-16 ENVIRONMENTAL CONTROLS TRAINING

Control: The organization trains personnel in the use of environmental controls (e.g., power, temperature and humidity, fire protection, lighting, plumbing).

Supplemental Guidance: None.

Control Enhancements: None.

PE-17 ENVIRONMENTAL CONTROLS TESTING

Control: The organization tests the environmental controls (e.g., power, temperature and humidity, fire protection, lighting, plumbing) within the facility where the information system resides [*Assignment: organization-defined time period for each type of test conducted in each facility*], assesses the test results, takes corrective actions where needed, and maintains test records.

Supplemental Guidance: None.

Control Enhancements: None.

PE-18 DELIVERY AND REMOVAL

Control: The organization controls information system-related items (i.e., hardware, firmware, software) 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 access. Appropriate organizational officials authorize the delivery or removal of information system-related items belonging to the organization.

Control Enhancements: None.

PE-19 ALTERNATE WORK SITE

Control: Individuals within the organization employ appropriate information system security controls at alternate work sites.

Supplemental Guidance: NIST Special Publication 800-46 provides guidance on security in telecommuting and broadband communications. The organization provides a means for employees to communicate with information system security staff in case of security problems.

Control Enhancements: None.

Draft

PE-20 ACCESS CONTROL FOR PORTABLE AND MOBILE SYSTEMS

Control: The organization controls physical access to portable and mobile information systems.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs cryptography to protect information residing on portable and mobile information systems.

Draft

FAMILY: PLANNING (PL)

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, 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 federal laws, directives, policies, regulations, standards, and guidance. The security planning policy 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.

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: NIST Special Publication 800-18 provides guidance on security planning. Information system security plans are consistent with the intent of Special Publication 800-18.

Control Enhancements: None.

PL-3 SYSTEM SECURITY PLAN UPDATE

Control: The organization reviews the security plan for the information system [*Assignment: organization-defined time period*] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.

Supplemental Guidance: None.

Control Enhancements: None.

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 system usage. The organization receives written acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, prior to authorizing access to the information system.

Supplemental Guidance: NIST Special Publication 800-18 provides guidance on preparing rules of behavior.

Control Enhancements: None.

Draft

PL-5 PRIVACY IMPACT ASSESSMENT

Control: The organization conducts a privacy impact assessment on the information system.

Supplemental Guidance: OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of FISMA.

Control Enhancements: None.

Draft

FAMILY: PERSONNEL SECURITY (PS)

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, 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 federal laws, 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.

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 every [*Assignment: organization-defined time period*].

Supplemental Guidance: Position risk designations are consistent with [5 CFR 731.106(a)] and Office of Personnel Management policy and guidance.

Control Enhancements: None.

PS-3 PERSONNEL SCREENING

Control: The organization screens individuals requiring access to organizational information and information systems prior to authorizing access.

Supplemental Guidance: Screening is consistent with the criteria established for the risk designation of the assigned position. Organizations consider appropriate sources of information for the screening process in accordance with Office of Personnel Management policy and guidance. These sources include National Agency Check Investigations, Minimum Background Investigations, Limited Background Investigations, Background Investigations, Periodic Reinvestigations, and Periodic Reinvestigations-Resident.

Control Enhancements: None.

PS-4 PERSONNEL TERMINATION

Control: When employment is terminated, the organization terminates information system access, conducts exit interviews, ensures the return of all organizational information system-related property (e.g., keys, identification cards, building passes), and ensures access to official records created by the employee that are stored on organizational information systems.

Supplemental Guidance: None.

Control Enhancements: None.

Draft

PS-5 PERSONNEL TRANSFER

Control: The organization reviews information systems/facilities access authorizations when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations).

Supplemental Guidance: None.

Control Enhancements: None.

PS-6 ACCESS AGREEMENTS

Control: The organization completes appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems prior to authorizing access.

Supplemental Guidance: None.

Control Enhancements: None.

PS-7 THIRD-PARTY PERSONNEL SECURITY

Control: The organization establishes personnel security requirements for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management) and monitors provider compliance to ensure adequate security.

Supplemental Guidance: The organization explicitly expresses personnel security requirements in acquisition-related documents. NIST Special Publication 800-35 provides guidance on information technology security services.

Control Enhancements: None.

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 federal laws, 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.

Draft

FAMILY: RISK ASSESSMENT (RA)

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, 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 federal laws, 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.

RA-2 SECURITY CATEGORIZATION

Control: The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199 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: NIST Special Publication 800-60 provides guidance on determining the security categories of the information types resident on the information system. The organization conducts 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.

Control Enhancements: None.

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.

Supplemental Guidance: Risk assessments take into account all that is known about 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. NIST Special Publication 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments.

Control Enhancements: None.

Draft

RA-4 RISK ASSESSMENT UPDATE

Control: The organization updates the risk assessment [*Assignment: organization-defined time period*] 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.

Draft

FAMILY: SYSTEM AND SERVICES ACQUISITION (SA)

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

Supplemental Guidance: The system and services acquisition policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services 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.

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.

SA-3 LIFE CYCLE SUPPORT

Control: The organization manages the information system using a system development life cycle methodology.

Supplemental Guidance: NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle.

Control Enhancements: None.

Draft

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.

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; (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 800-53 provides guidance on recommended security controls for federal information systems to meet minimum security requirements for information systems categorized in accordance with FIPS 199. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-36 provides guidance on the selection of information security products. NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle.

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. NIST Special Publication 800-70 provides guidance on configuration settings for information technology products.

Control Enhancements: None.

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control: The organization ensures that adequate documentation for the information system and its constituent components is available, protects the documentation when required, and distributes the documentation to authorized personnel.

Supplemental Guidance: Administrator and user guides include information on: (i) configuring, installing, and operating the information system; and (ii) optimizing the system's security features.

Control Enhancements: None.

SA-6 SOFTWARE USAGE RESTRICTIONS

Control: The organization complies with software usage restrictions.

Supplemental Guidance: Software and associated documentation is 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.

SA-7 USER INSTALLED SOFTWARE

Control: The organization enforces explicit rules governing the downloading and installation of software by users.

Supplemental Guidance: If provided the necessary privileges, users have the ability to download and install no-cost software. The organization identifies what types of software downloads and installations are permitted (e.g., updates and security patches to existing software) and types of downloads and installations that are always prohibited (e.g., software that is free only for personal, not government, use).

Control Enhancements:

(1) The organization prohibits the installation of software by individuals other than authorized information system or security administrators.

SA-8 SECURITY DESIGN 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.

Control Enhancements: None.

SA-9 OUTSOURCED INFORMATION SYSTEM SERVICES

Control: The organization ensures that third-party providers of information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, and guidance. The organization monitors security control compliance.

Supplemental Guidance: Third-party providers are subject to the same information system security policies and procedures of the supported organization, and must conform to the same security control and documentation requirements as would apply to the organization's internal systems. Appropriate organizational officials approve outsourcing of information system services to third-party providers (e.g., service bureaus, contractors, and other organizations). The outsourced information system services documentation includes government, service provider, and end user security roles and responsibilities. NIST Special Publication 800-35 provides guidance on information technology security services.

Control Enhancements: None.

Draft

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION (SC)

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, 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 federal laws, 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.

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.

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 further divides the security functions with the functions enforcing access and information flow control isolated and protected from both nonsecurity functions and from other security functions.

(3) The information system minimizes the amount of nonsecurity functions included within the isolation boundary containing security functions.

(4) The information system security maintains its security functions in largely independent modules that avoid unnecessary interactions between modules.

(5) The information system security maintains its security functions in a layered structure minimizing interactions between layers of the design.

Draft

SC-4 INFORMATION REMNANTS

Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance: Control of information system remnants, sometimes referred to as object reuse, 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.

SC-5 DENIAL OF SERVICE PROTECTION

Control: The information system protects against the following denial of service attacks: [*Assignment: organization-defined list of attacks or reference to source for current list*].

Supplemental Guidance: The organization addresses, at a minimum, the denial of service vulnerabilities described in the I-CAT database (http://icat.nist.gov).

Control Enhancements:

(1) The information system protects against all applicable, publicly known denial of service attacks.

SC-6 RESOURCE PRIORITY

Control: The information system limits the use of resources by priority.

Supplemental Guidance: Priority protection ensures that a lower-priority process is not able to interfere with the information system servicing any higher-priority process.

Control Enhancements: None.

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 controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels). The operational failure of the boundary protection mechanisms does not result in any unauthorized release of information outside of the information system boundary. Information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site.

Control Enhancements:

(1) The organization physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces. The organization prevents public access into the organization's internal networks.

SC-8 TRANSMISSION INTEGRITY

Control: The information system protects the integrity of transmitted information.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs strong cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures.

Draft

SC-9 TRANSMISSION CONFIDENTIALITY

Control: The information system protects the confidentiality of transmitted information.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs strong cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless protected by alternative physical measures.

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: None.

Control Enhancements: None.

SC-11 TRUSTED PATH

Control: The information system establishes a trusted communications path between the user and the security functionality of the system.

Supplemental Guidance: None.

Control Enhancements: None.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.

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.

SC-13 CRYPTOGRAPHIC OPERATIONS

Control: The information system performs all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in FIPS-approved or NIST-recommended modes of operation.

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.

SC-14 PUBLIC ACCESS PROTECTIONS

Control: For publicly available systems, the information system protects the integrity of the information and applications.

Supplemental Guidance: None.

Control Enhancements: None.

Draft

SC-15 COLLABORATIVE COMPUTING

Control: The information system prohibits remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provides an explicit indication of use to the local users (e.g., use of camera or microphone).

Supplemental Guidance: None.

Control Enhancements:

(1) The information system provides physical disconnect of camera and microphone in a manner that supports ease of use.

SC-16 TRANSMISSION OF SECURITY PARAMETERS

Control: The information system reliably associates security parameters (e.g., security labels and markings) with information exchanged between information systems.

Supplemental Guidance: None.

Control Enhancements: None.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control: The organization develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.

Supplemental Guidance: Registration to receive a public key certificate includes authorization by a supervisor or a responsible official, and is done by a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party. NIST Special Publication 800-63 provides guidance on electronic authentication.

Control Enhancements: None.

SC-18 MOBILE CODE

Control: The organization restricts the deployment of mobile code based on its potential to cause damage to the information system if used maliciously. Appropriate organizational officials authorize the use of mobile code.

Supplemental Guidance: Control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the information system.

Control Enhancements: None.

Draft

FAMILY: SYSTEM AND INFORMATION INTEGRITY (SI)

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, 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 federal laws, 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.

SI-2 FLAW REMEDIATION

Control: The organization identifies, reports, and corrects information system flaws.

Supplemental Guidance: The organization identifies information systems affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems prior to installation. NIST Special Publication 800-40 provides guidance on security patch installation.

Control Enhancements:

(1) The organization centrally manages the flaw remediation process and installs updates automatically without individual user intervention.

(2) The organization employs automated mechanisms to periodically and upon command determine the state of information system components with regard to flaw remediation.

SI-3 MALICIOUS CODE PROTECTION

Control: The information system implements malicious code protection that includes a capability for automatic updates.

Supplemental Guidance: The organization employs antiviral mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at each workstation, server, or mobile computing device on the network. The organization uses the antiviral mechanisms to detect and eradicate malicious code transported by electronic mail, electronic mail attachments, removable media (e.g., diskettes or compact disks) or other methods. The organization updates antiviral mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. Consideration is given to using antiviral software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations).

Control Enhancements:

(1) The organization centrally manages malicious code protection mechanisms.

(2) The information system automatically updates antiviral mechanisms.

SI-4 INTRUSION DETECTION 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: Intrusion detection and information system monitoring capability can be achieved through a variety of tools and techniques (e.g., intrusion detection systems, antiviral software, log monitoring software, network forensic analysis tools).

Control Enhancements:

(1) The organization networks 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 in support of detecting system-level attacks.

(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.

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.

Control Enhancements:

(1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

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: None.

Control Enhancements:

(1) The organization employs automated mechanisms to provide centralized notification of failed security tests.

(2) The organization employs automated mechanisms to support centralized management of distributed security testing.

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: None.

Draft

APPENDIX G

SECURITY CONTROL MAPPINGS

RELATIONSHIP OF SECURITY CONTROLS TO OTHER STANDARDS AND CONTROL SETS

The mapping table in this appendix provides organizations with a general indication of Special Publication 800-53 security control coverage with respect to other frequently referenced security control standards and control sets.[17] 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 searching for a similar security topic in the other referenced security control standards and control sets. Security controls with similar functional meaning (e.g., Special Publication 800-53 contingency planning and ISO/IEC 17799 business continuity) are included in the mapping table. In some instances, similar topics are addressed in the security control sets but provide a different context, perspective, or scope (e.g., Special Publication 800-53 addresses privacy requirements in terms of privacy policy notification, whereas ISO/IEC 17799 addresses privacy requirements in terms of legislation and regulations). Organizations are encouraged to use the mapping table as a starting point for conducting further analysis and interpretation of control similarity and associated coverage when comparing disparate control sets.

Draft

[17] The security control mapping table includes references to: (i) ISO/IEC 17799:2000, *Code of Practice for Information Security Management*; (ii) NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*; and (iii) GAO, *Federal Information System Controls Audit Manual*. The numerical designations in the respective columns indicate the paragraph number(s) in the above documents where the security controls, control objectives, or associated implementation guidance may be found.

CONTROL NUMBER	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM
Access Control				
AC-1	Access Control Policy and Procedures	9.1.1 9.4.1	15. 16.	---
AC-2	Account Management	9.2.1 9.2.2	6.1.8 15.1.1 15.1.4 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
AC-3	Access and Information Flow Control	9.2.4 9.4.6 9.4.8	15.1.1 16.1.1 16.1.2 16.1.3 16.1.7 16.1.9 16.2.7 16.2.10 16.2.11	AC-2 AC-3.2
AC-4	Separation of Duties	8.1.4	6.1.1 6.1.2 6.1.3 15.2.1 16.1.2 17.1.5	AC-3.2 SD-1.2
AC-5	Least Privilege	9.2.2	16.1.2 16.1.3 17.1.5	AC-3.2
AC-6	Unsuccessful Logon Attempts	9.5.2	15.1.14	AC-3.2
AC-7	System Use Notification	9.5.2	16.2.13	AC-3.2
AC-8	Privacy Policy Notification	12.1.4	16.3.1	AC-3.2
AC-9	Previous Logon Notification	9.5.2	---	AC-3.2
AC-10	Concurrent Session Control	---	---	---
AC-11	Session Lock	---	16.1.4	AC-3.2
AC-12	Session Termination	9.5.7	16.1.4 16.2.6	AC-3.2
AC-13	Supervision and Review—Access Control	9.2.4	7.1.10 11.2.2 16.1.10 17.1.6 17.1.7	AC-4 AC-4.3 SS-2.2
AC-14	Permitted Actions without Identification or Authentication	---	16.2.12	---
AC-15	Automated Marking	5.2.2	8.2.4 16.1.6	AC-3.2
AC-16	Automated Labeling	5.2.2	16.1.6	AC-3.2
AC-17	Remote Access	9.4.3 9.4.4	16.2.12 16.2.4 16.2.8	AC-3.2
AC-18	Wireless Access Restrictions	---	---	---
Awareness and Training				
AT-1	Security Awareness and Training Policy and Procedures	---	13.	---

Draft

CONTROL NUMBER	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM
AT-2	Security Awareness	6.3.1 9.8.1 11.1.4 12.1.4	13.1.4	---
AT-3	Security Training	4.2.2 6.2.1 6.3.1 8.3.1 9.8.1	13.1	---
AT-4	Security Training Records	---	13.1.2	---
Audit and Accountability				
AU-1	Audit and Accountability Policy and Procedures	---	17.	---
AU-2	Auditable Events	11.1.2	17.1.1 17.1.2 17.1.4	---
AU-3	Content of Audit Records	9.7.2	17.1.1	---
AU-4	Audit Storage Capacity	9.7.2	---	---
AU-5	Audit Processing	9.7.2	---	---
AU-6	Audit Monitoring, Analysis, and Reporting	9.7.2	17.1.7 17.1.8	AC-4.3
AU-7	Audit Reduction and Report Generation	---	17.1.2 17.1.7	---
AU-8	Time Stamps	9.7.3	---	---
AU-9	Protection of Audit Information	12.3.2	17.1.3 17.1.4	---
AU-10	Non-repudiation	10.3.4	17.1.1	---
Certification, Accreditation, and Security Assessments				
CA-1	C&A and Security Assessment Policy and Procedures	---	2. 4.	---
CA-2	Security Assessment	4.1.7	2.1.1 2.1.2 2.1.3 2.1.4	SP-5.1
CA-3	Information System Connections	---	3.2.9 4.1.2 4.1.8 12.2.3	CC-2.1
CA-4	Security Certification	---	3.2.3 3.2.5 4.1.1 4.1.6 11.2.8 12.2.5	CC-2.1
CA-5	Plan of Action and Milestones	---	2.2.1 4.2.1	SP-5.1 SP-5.2
CA-6	Security Accreditation	---	4.1.1 4.1.7 4.1.8 12.2.5	---
CA-7	Continuous Monitoring	9.7.2 12.2.1	10.2.1	---

Draft

CONTROL NUMBER	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM
Configuration Management				
CM-1	Configuration Management Policy and Procedures	---	---	---
CM-2	Baseline Configuration	---	10.1.4 10.2.7 10.2.8 10.2.9	CC-2.3 CC-3.1 SS-1.2
CM-3	Configuration Change Control	8.1.2 10.4.1 10.5.1	10.2.2 10.2.3 10.2.10 10.2.11	SS-3.2 CC-2.2
CM-4	Monitoring Configuration Changes	8.1.2	10.2.1 10.2.4	SS-3.1 SS-3.2 CC-2.1
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
CM-6	Configuration Settings	---	10.2.6	---
Contingency Planning				
CP-1	Contingency Planning Policy and Procedures	3.1.1	9.	---
CP-2	Contingency Plan	11.1.3	4.1.4 9.1.1 9.2 9.2.1 9.2.2 9.2.3 9.2.10	SC-3.1 SC-1.1
CP-3	Contingency Training	11.1.3 11.1.4	9.3.2	SC-2.3
CP-4	Contingency Plan Testing	11.1.5	4.1.4 9.3.3	SC-3.1
CP-5	Contingency Plan Update	11.1.5	9.3.1 9.3.3 10.2.12	SC-2.1 SC-3.1
CP-6	Alternate Storage Sites	8.4.1	9.2.4 9.2.5 9.2.7 9.2.9	SC-2.1 SC-3.1
CP-7	Alternate Processing Sites	11.1.4	9.2.4 9.2.5 9.2.7 9.2.9	SC-2.1 SC-3.1
CP-8	Alternate Telecommunications Services	11.1.4	---	---
CP-9	Information System Backup	8.4.1	9.2.6 9.2.9	SC-2.1
CP-10	Information System Recovery and Reconstitution	11.4.1	9.2.8	SC-2.1
Identification and Authentication				
IA-1	Identification and Authentication Policy and Procedures	---	15.	---
IA-2	User Identification and Authentication	9.5.3	15.1	---
IA-3	Device Authentication and Authentication	9.4.4 9.5.1 9.8.1	16.2.7	---

Draft

CONTROL NUMBER	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM
IA-4	Identifier Management	9.5.3	15.1.1 15.2.2 16.1.5 15.1.8	AC-2.1 AC-3.2 SP-4.1
IA-5	Authenticator Management	---	15.1.7 15.1.10 15.1.11 15.1.12 15.1.13	AC-3.2
IA-6	Authenticator Feedback	---	---	---
IA-7	Cryptographic Module Authentication	---	16.1.7	---
Incident Response				
IR-1	Incident Response Policy and Procedures	3.1.1	14.	---
IR-2	Incident Response Training	6.3.1	14.1.4	SP-3.4
IR-3	Incident Response Testing	---	---	---
IR-4	Incident Handling	8.1.3	14.1.1 14.1.2 14.1.6	SP-3.4
IR-5	Incident Monitoring	8.1.3	14.1.3	---
IR-6	Incident Reporting	8.1.3	14.1.1 14.1.2 14.1.3 14.2.3	---
IR-7	Incident Response Assistance	---	8.1.1 14.1.1	SP-3.4
Maintenance				
MA-1	System Maintenance Policy and Procedures	8.1.1	10.	---
MA-2	Periodic Maintenance	7.2.4	10.1.1 10.1.3 10.2.1	SS-3.1
MA-3	Maintenance Tools	---	10.1.3 11.2.4	---
MA-4	Remote Maintenance	9.4.5	10.1.1	SS-3.1
MA-5	Maintenance Personnel	7.2.4	10.1.1 10.1.3	SS-3.1
MA-6	Timely Maintenance	---	9.1.2	SC-1.2
Media Protection				
MP-1	Media Protection Policy and Procedures	8.6.1	8.	---
MP-2	Media Access	8.6.1	8.2.1 8.2.2 8.2.6 8.2.7	---
MP-3	Media Labeling	---	8.2.5 8.2.6 10.2.9	---
MP-4	Media Storage	8.6.3 12.3.1	7.1.4 8.2.1 8.2.2	AC-3.1
MP-5	Media Transport	8.7.2	8.2.2 8.2.4	---

Draft

CONTROL NUMBER	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM
MP-6	Media Sanitization	8.6.1	3.2.12 3.2.13 8.2.8	AC-3.4
MP-7	Media Destruction and Disposal	7.2.6 8.6.2	3.2.12 3.2.13 8.2.10	AC-3.4
MP-8	Media-related Records	---	3.2.13 7.1.3 8.2.3 8.2.7	AC-3.1 AC-3.4
Physical and Environmental Protection				
PE-1	Physical and Environmental Protection Policy and Procedures	---	7.	
PE-2	Physical Access Authorizations	---	7.1.1 7.1.2	AC-3.1
PE-3	Physical Access Control	7.1.2 7.1.5	7.1.1 7.1.2 7.1.5 7.1.6	AC-3.1
PE-4	Access Control for Transmission Medium	---	7.2.2	---
PE-5	Access Control for Display Medium	---	7.2.1	---
PE-6	Monitoring Physical Access	7.2.3	7.1.9	AC-4
PE-7	Visitor Control	7.1.2	7.1.7	AC-3.1
PE-8	Access Logs	7.1.2	7.1.9	AC-4
PE-9	Power Equipment and Cabling	7.2.3	7.1.16	SC-2.2
PE-10	Emergency Shutoff	7.2.2	---	---
PE-11	Emergency Power	7.2.2	7.1.18	SC-2.2
PE-12	Emergency Lighting	7.2.2	---	---
PE-13	Fire Protection	7.2.1	7.1.12	SC-2.2
PE-14	Temperature and Humidity Controls	---	7.1.14 7.1.15	SC-2.2
PE-15	Water Damage Protection	7.2.1	7.1.17	SC-2.2
PE-16	Environmental Controls Training	---	---	---
PE-17	Environmental Controls Testing	---	---	---
PE-18	Delivery and Removal	7.1.5	7.1.3 7.1.11	AC-3.1
PE-19	Alternate Work Site	9.8.2	---	---
PE-20	Access Control for Portable and Mobile Systems	9.8.1	7.3.2	---
Planning				
PL-1	Security Planning Policy and Procedures	---	5.	---
PL-2	System Security Plan	---	5.1.1 5.1.2	SP-2.1
PL-3	System Security Plan Update	---	5.2.1	SP-2.1
PL-4	Rules of Behavior	---	4.1.3	---
PL-5	Privacy Impact Assessment	12.1.4	---	---

Draft

CONTROL NUMBER	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM
Personnel Security				
PS-1	Personnel Security Policy and Procedures	---	6.	---
PS-2	Position Categorization	---	6.1.1 6.1.2	SD-1.2
PS-3	Personnel Screening	6.1.2	6.2.1 6.2.2 6.2.3 6.2.4	SP-4.1
PS-4	Personnel Termination	---	6.1.7	SP-4.1
PS-5	Personnel Transfer	---	6.1.7	SP-4.1
PS-6	Access Agreements	6.1.3	6.2.2	SP-4.1
PS-7	Third-Party Personnel Security	4.2.2	6.2.2	SP-4.1
PS-8	Personnel Sanctions	6.3.5 9.2.1	---	---
Risk Assessment				
RA-1	Risk Assessment Policy and Procedures	---	1.	---
RA-2	Security Categorization	5.2.1	1.1.3 3.1.1	SP-1 AC-1.1 AC-1.2
RA-3	Risk Assessment	INTRO	1.1.2 1.1.4 1.1.5 1.1.6	SP-1
RA-4	Risk Assessment Update	INTRO	1.1.2	SP-1
System and Services Acquisition				
SA-1	System and Services Acquisition Policy and Procedures	---	3.	---
SA-2	Allocation of Resources	8.2.1	3.1.2 3.1.3 3.1.5	---
SA-3	Life Cycle Support	---	3.1	---
SA-4	Acquisitions	10.1.1	3.1.6 3.1.7 3.1.9 3.1.11 3.1.12	---
SA-5	Information System Documentation	8.6.4	3.2.2 3.2.3 3.2.4 3.2.8	CC-2.1
SA-6	Software Usage Restrictions	12.1.2	10.2.10 10.2.13	SS-3.2 SP-2.1
SA-7	User Installed Software	10.4.1	10.2.10	SS-3.2
SA-8	Security Design Principles	---	---	---
SA-9	Outsourced Information System Services	4.2.1	12.2.3	---
System and Communications Protection				
SC-1	System and Communications Policy and Procedures	---	---	---
SC-2	Application Partitioning	---	---	---
SC-3	Security Function Isolation	---	---	---

Draft

CONTROL NUMBER	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM
SC-4	Information Remnants	---	3.2.12	AC-3.4
SC-5	Denial of Service Protection	8.1.3	---	---
SC-6	Resource Priority	---	9.1.3 11.2.7	SC-1.3
SC-7	Boundary Protection	9.4.6	16.2.2 16.2.7 16.2.8 16.2.9 16.2.10 16.2.11 16.2.14	AC-3.2
SC-8	Transmission Integrity	8.7.3	11.2.1 11.2.4 11.2.9 16.2.14	AC-3.2
SC-9	Transmission Confidentiality	---	---	---
SC-10	Network Disconnect	---	16.2.6	AC-3.2
SC-11	Trusted Path	---	---	---
SC-12	Cryptographic Key Establishment and Management	10.3.5	16.1.7 16.1.8	---
SC-13	Cryptographic Operations	---	16.1.7 16.1.8	---
SC-14	Public Access Protections	8.7.6	16.3.1	---
SC-15	Collaborative Computing	---	---	---
SC-16	Transmission of Security Parameters	5.2.2 8.7.1	16.1.6	AC-3.2
SC-17	Public Key Infrastructure Certificates	10.3.5	---	---
SC-18	Mobile Code	---	---	---
System and Information Integrity				
SI-1	System and Information Integrity Policy and Procedures	---	11.	---
SI-2	Flaw Remediation	10.4.1	10.3.2 11.1.1 11.1.2 11.2.2 11.2.7	SS-2.2
SI-3	Malicious Code Protection	8.3.1	11.1.1 11.1.2	---
SI-4	Intrusion Detection Tools and Techniques	9.7.2	11.2.5 11.2.6	---
SI-5	Security Alerts and Advisories	---	14.1.1 14.1.2 14.1.5	SP-3.4
SI-6	Security Functionality Verification	---	11.2.1 11.2.2	SS-2.2
SI-7	Software and Information Integrity	10.2.1 10.2.2 10.2.4	11.2.1 11.2.4	---

Draft