NIST Special Publication 800-53
Revision 3

Recommended Security Controls for Federal Information Systems and Organizations

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

INFORMATION SECURITY

INITIAL PUBLIC DRAFT

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

February 2009

U.S. Department of Commerce
Otto J. Wolff, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Deputy 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.

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements, for federal agencies, 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 Circular A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in Circular A-130, Appendix III.

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

NIST Special Publication 800-53, Revision 3, 209 pages

(February 2009)

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 NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

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

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

Public comment period: February 5 through March 27, 2009

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Electronic mail: sec-cert@nist.gov

Compliance with NIST Standards and Guidelines

NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing FISMA and managing cost-effective information security programs to protect the information and information systems supporting organizational operations and assets, individuals, other organizations, and the Nation.

- Federal Information Processing Standards (FIPS) are developed and issued by NIST in accordance with FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. FISMA requires that federal agencies comply with these standards, and therefore, agencies may not waive their use.
- Special Publications (SP) are developed and issued by NIST as recommendations and guidance documents. OMB policies (including OMB FISMA Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management), state that for other than national security programs and systems, federal agencies must follow NIST guidance.[1]
- Other security-related publications, including interagency and internal reports (NISTIRs), and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when specified by OMB.

Schedule for Compliance with NIST Standards and Guidelines

- For legacy information systems, federal agencies[2] are expected to be in compliance with NIST security standards and guidelines within one year of the publication date unless otherwise directed by OMB or NIST.[3]
- For information systems under development, agencies are expected to be in compliance with NIST security standards and guidelines immediately upon deployment of the system.

[1] While federal agencies are required to follow NIST guidance in accordance with OMB policy, there is flexibility in how agencies apply the guidance. Federal agencies should apply the security concepts and principles articulated in the NIST guidance in accordance with and in the context of the agency's missions, business functions, and environment of operation. Consequently, the application of NIST guidance by federal agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of *adequate security* for federal information systems. When assessing federal agency compliance with NIST guidance, Inspectors General, evaluators, auditors, and assessors, should consider the intent of the security concepts and principles articulated within the specific guidance document and how the agency applied the guidance in the context of its mission/business responsibilities, operational environment, and unique organizational conditions.

[2] The term *agency* is used in this publication in lieu of the more general term *organization* only in those circumstances where its usage is directly related to other source documents such as federal legislation or policy.

[3] The one-year compliance date for revisions to NIST Special Publications applies only to the new and/or updated material in the publications resulting from the periodic revision process. Agencies are expected to be in compliance with previous versions of NIST Special Publications within one year of the publication date of the previous versions.

Acknowledgments

The authors, Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, and George Rogers, wish to thank their colleagues who reviewed drafts of this publication and contributed to its development. A special note of thanks goes to Peggy Himes and Elizabeth Lennon for their superb technical editing and administrative support, to Kelley Dempsey, Pat Toth, Murugiah Souppaya, Kevin Stine, Matt Barrett, Steve Quinn, Bill MacGregor, Christian Enloe, Karen Scarfone, Bill Burr, Doug Montgomery, Scott Rose, Mark Wilson, and Erika McCallister for their review of the security controls and insightful recommendations, and to Annabelle Lee for her contribution to earlier versions of the document. In addition, the authors wish to recognize Rich Graubart, Marshall Abrams, Harriett Goldman, John Woodward, Karen Quigg, Peter Gouldmann, Bennett Hodge, Roger Johnson, Sarbari Gupta, Dennis Bailey, Richard Wilsher, Nadya Bartol, and Tom Madden for their exceptional contributions in helping to improve the content of the publication. The authors also gratefully acknowledge and appreciate the many contributions from individuals in the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

A special acknowledgment is also given to the participants in the *Industrial Control System (ICS) Security Project* who have put forth significant effort in helping to augment the security controls in NIST Special Publication 800-53 for industrial controls systems. These participants include: Keith Stouffer (NIST), Stu Katzke (NIST), and Marshall Abrams (MITRE Corporation) from the ICS Security Project Development Team; federal agencies participating in the ICS workshops; and individuals and organizations from the public and private sector ICS community providing thoughtful and insightful comments on the proposed augmentations.

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

IMPLEMENTING INFORMATION SECURITY STANDARDS AND GUIDELINES

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory, federal standard developed by NIST in response to FISMA. To comply with the federal standard, organizations must first determine the security category of their information system in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and then apply the appropriately tailored set of baseline security controls in NIST Special Publication 800-53, *Security Controls for Federal Information Systems and Organizations*. Organizations have flexibility in applying the baseline security controls in accordance with the guidance provided in Special Publication 800-53. This allows organizations to select security controls that more closely align with their mission and business requirements and environments of operation.

FIPS 200 and NIST Special Publication 800-53, in combination, help ensure that appropriate security requirements and security controls are applied to all federal information and information systems. An organizational assessment of risk validates the initial security control selection and determines if any additional controls are needed to protect organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. The resulting set of agreed-upon security controls establishes a level of security due diligence for the organization.

In addition to the security requirements established by FISMA, there may also be specific security requirements in different mission/business areas within organizations that are governed by other laws, Executive Orders, directives, policies, regulations, or associated governing documents, (e.g., the Health Insurance Portability and Accountability Act of 1996, the Federal Financial Management Improvement Act of 1996, or OMB Circular A-127 on Financial Management Systems). These security requirements may not be equivalent to the security requirements established by FISMA or the requirements may enhance or further refine the FISMA requirements. Organizational officials (e.g., authorizing officials, chief information officers, senior agency information security officers, information system owners, information system security officers, and procurement officials) take necessary actions to help ensure that: (i) information security requirements are addressed in all acquisitions of federal information systems, system components, and information system services; and (ii) required security controls are implemented in organizational information systems. See http://csrc.nist.gov/sec-cert/ca-compliance.html for additional information on FISMA compliance.

DEVELOPING COMMON INFORMATION SECURITY FOUNDATIONS

COLLABORATION AMONG PUBLIC AND PRIVATE SECTOR ENTITIES

In developing standards and guidelines required by FISMA, NIST consults with other federal agencies and offices as well as the private sector to improve information security, avoid unnecessary and costly duplication of effort, and ensure that NIST publications are complementary with the standards and guidelines employed for the protection of national security information and systems. In addition to its comprehensive public review and vetting process, NIST is collaborating with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DOD), and the Committee on National Security Systems (CNSS) to establish a common foundation for information security across the federal government. This common foundation for information security will provide the Intelligence, Defense, and Civil sectors of the federal government and their support contractors, more uniform and consistent ways to manage the risk to organizational operations and assets, individuals, other organizations, and the Nation that results from the operation and use of information systems. NIST is also working with public and private sector entities to establish specific mappings and relationships between the security standards and guidelines developed by NIST and the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27001, Information Security Management System (ISMS).

Notes to Reviewers

This is the first major update of NIST Special Publication 800-53 since its initial publication in December 2005. We have received excellent feedback from our customers during the past three years and have taken this opportunity to provide significant improvements to the security control catalog. In addition, the changing threat environment and growing sophistication of cyber attacks necessitated specific changes to the allocation of security controls and control enhancements in the low-impact, moderate-impact, and high-impact baselines. We also continue to work closely with the Department of Defense and the Office of the Director of National Intelligence under the auspices of the Committee on National Security Systems on the harmonization of security control specifications across the federal government. And lastly, we have added new security controls to address organization-wide security programs and introduced the concept of a security program plan to capture security program management requirements for organizations. The privacy-related material, originally scheduled to be included in Special Publication 800-53, Revision 3, will undergo a separate public review process in the near future and be incorporated into this publication, when completed.

The specific changes in Special Publication 800-53, Revision 3 include:

- Restructuring of security controls to include specific requirements previously stated in Supplemental Guidance;
- Adjusting security control/control enhancement allocations to security control baselines;
- Eliminating security controls and control enhancements that are redundant or no longer needed;
- Incorporating the revised, simplified, six-step Risk Management Framework;
- Strengthening selected security controls by adding new security control enhancements;
- Adding security program management controls that affect organizations, at large, including areas such as capital planning and budgeting, enterprise architecture, and risk management;
- Providing additional guidance on the management of common controls within organizations;
- Adding security controls and control enhancements for advanced cyber threats, including supply chain threats;
- Introducing a three-part strategy for harmonizing the FISMA security standards and guidelines with international security standards including an updated mapping table for security controls in ISO/IEC 27001 (Annex A); and
- Updating supporting appendices including references, glossary, and acronyms.

Your feedback to us, as always, is important. We appreciate each and every contribution from our reviewers. The very insightful comments from both the public and private sectors continue to help shape our publications and ensure that they are meeting the needs of our customers.

-- Ron Ross
FISMA Implementation Project Leader

Table of Contents

CHAPTER ONE

INTRODUCTION

THE NEED FOR SECURITY CONTROLS TO PROTECT INFORMATION AND INFORMATION SYSTEMS

The selection and implementation of appropriate *security controls* for an information system[4] are important tasks that can have major implications on the operations[5] and assets of an organization[6] as well as the welfare of individuals and the Nation. 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 mitigate the risk incurred by the use of information and information systems in the execution of organizational missions and business functions?
- Have the selected security controls been implemented or is there a realistic plan for their implementation?
- What is the desired or required level of assurance (i.e., grounds for confidence) that the selected security controls, as implemented, are effective[7] 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, mitigates as deemed necessary, and monitors on an ongoing basis, risks[8] arising from its information and information systems.[9] The security controls defined in Special Publication 800-53 (as amended) and recommended for use by organizations in protecting their information systems should be employed in conjunction with and as part of a well-defined and documented information security program. The information security program management controls described in Appendix G, complement the security controls for an information system described in Appendix F by focusing on the organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs.

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

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

[6] The term *organization* describes an entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).

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

[8] Risk is a function of likelihood of occurrence and the degree of harm to organizational operations, organizational assets, individuals, other organizations, and the Nation.

[9] The E-Government Act (P.L. 107-347) recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.

It is of paramount importance that responsible officials within the organization understand the risks and other factors that could adversely affect organizational operations, organizational assets, individuals, other organizations, and the Nation. These officials must also understand the current status of their security programs and the security controls planned or in place to protect their information and 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 and business functions with what the Office of Management and Budget (OMB) Circular A-130 defines as *adequate security*, or security commensurate with risk 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. This includes guidelines for meeting the requirements of FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. The guidelines apply to all components[10] of an information system that process, store, or transmit federal information. The guidelines have been developed to help achieve more secure information systems and effective risk management within the federal government by:

- Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems and organizations;
- Providing a recommendation for minimum security controls for information systems categorized in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*;
- Providing a stable, yet flexible catalog of security controls for information systems and organizations to meet current organizational protection needs and the demands of future protection needs based on changing requirements and technologies; and
- Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness.

The guidelines provided in this special publication are applicable to all federal information systems[11] other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542. The guidelines have been broadly developed from a technical perspective to complement similar guidelines for national security systems and may be used for such systems with the approval of the Director of National Intelligence (DNI), the Secretary of Defense (SECDEF), or the Chairman of the Committee on National Security Systems (CNSS), or their designees. State, local, and tribal governments, as well as private sector organizations are encouraged to consider using these guidelines, as appropriate.

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

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

1.2 TARGET AUDIENCE

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

- Individuals with information system and information security management and oversight responsibilities (e.g., authorizing officials, chief information officers, senior information security officers,[12] information system managers, information security managers);
- Individuals with information system development responsibilities (e.g., program and project managers, information technology product developers, information system designers and developers, systems integrators);
- Individuals with information security implementation and operational responsibilities (e.g., mission/business owners, information system owners, common control providers, information owners/stewards, information system security engineers, information system administrators, information system security officers); and
- Individuals with information system and information security assessment and monitoring responsibilities (e.g., auditors, Inspectors General, system evaluators, assessors/assessment teams, independent verification and validation assessors, information system owners).

Commercial companies producing information technology products and systems, creating information security-related technologies, and providing information security services can also benefit from the information in this publication.

1.3 RELATIONSHIP TO OTHER SECURITY CONTROL PUBLICATIONS

To create a technically sound and broadly applicable set of security controls for information systems and organizations, 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. The objective of NIST Special Publication 800-53 is to provide a set of security controls that can satisfy the breadth and depth of security requirements[13] levied on information systems and organizations and that is consistent with and complementary to other established information security standards.

The catalog of security controls provided in Special Publication 800-53 can be effectively used to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements. It is the responsibility of organizations to select the appropriate security controls, to implement the controls correctly, and to demonstrate the effectiveness of the controls in satisfying their stated security requirements. The security controls in the catalog facilitate the development of assessment methods and procedures that can be used to demonstrate control effectiveness in a consistent and repeatable manner—thus contributing to the organization's confidence that there is ongoing compliance with its stated security requirements.[14]

[12] At the *agency* level, this position is known as the Senior Agency Information Security Officer (SAISO). Organizations subordinate to federal agencies may also refer to this position as the *Chief Information Security Officer*.

[13] 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.

[14] NIST Special Publication 800-53A provides guidance on assessing the effectiveness of security controls defined in this publication.

1.4 ORGANIZATIONAL RESPONSIBILITIES

Organizations[15] use FIPS 199 to define security categories for their information systems. Based on this categorization, organizations designate information systems as low-impact, moderate-impact or high-impact systems. For each information system, the recommendation for minimum security controls from Special Publication 800-53 (i.e., the *baseline* security controls defined in Appendix D, adjusted in accordance with the *tailoring* guidance in Section 3.3) is intended to be used as a starting point for and as input to the organization's risk assessment process.[16] While the FIPS 199 security categorization associates the operation of the information system with the potential adverse impact on organizational operations and assets, individuals, other organizations, and the Nation, the incorporation of refined threat and vulnerability information during the risk assessment facilitates the selection of additional security controls *supplementing* the tailored baseline to address specific organizational needs and tolerance for risk. The final, agreed-upon set of security controls is documented with appropriate rationale in the security plan for the information system.[17] The use of security controls from Special Publication 800-53 and the incorporation of tailored baseline controls as a starting point in the control selection process, facilitate a more consistent level of security across federal information systems and organizations. It also offers the needed flexibility to appropriately modify the controls based on specific organizational policies and requirements, particular conditions and circumstances, known threat and vulnerability information, and tolerance for risk.

Building more secure information systems is a multifaceted undertaking that involves the use of: (i) well-defined system-level security requirements and security specifications; (ii) well-designed information technology products; (iii) sound systems/security engineering principles and practices to effectively integrate information technology products into information systems; (iv) state-of-the-art methods for product/system assessment; and (v) comprehensive system security planning and life cycle management.[18] From a systems engineering viewpoint, security is just one of many required operational capabilities for an information system supporting organizational mission and business processes—capabilities that must be funded by the organization throughout the life cycle of the system in order to achieve mission/business success. It is important that the organization *realistically* assesses the risk to organizational operations and assets, individuals, other organizations, and the Nation that arises by placing the information system into operation or continuing its operation. In addition, information security requirements must be accomplished with full consideration of the risk management strategy[19] of the organization in light of the potential cost, schedule, and performance issues associated with the acquisition, deployment, and operation of the information system.

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

[16] Risk assessments can be accomplished in a variety of ways depending on the specific needs of the organization. NIST Special Publication 800-30 provides guidance on the assessment of risk as part of an overall risk management process.

[17] NIST Special Publication 800-18 provides guidance on documenting information system security controls. The guidance in Special Publication 800-18 is augmented by Special Publication 800-53 with a recommendation for rationale to be included in the security plan.

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

[19] NIST Special Publication 800-39 provides guidance on organization-wide risk management.

1.5 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the fundamental concepts associated with security control selection and specification including: (i) the structural components of security controls and how the controls are organized into families; (ii) security control baselines; (iii) the use of common security controls in support of organization-wide information security programs; (iv) security controls in external environments; (v) assurance in the effectiveness of security controls; and (vi) the commitment to maintain currency of the individual security controls and the control baselines.
- **Chapter Three** describes the process of selecting and specifying security controls for an information system including: (i) defining the organization's overall approach to managing risk; (ii) categorizing the system in accordance with FIPS 199; (iii) selecting and tailoring the initial set of baseline security controls; (iv) supplementing the tailored security control baseline, as necessary, based upon risk assessment results; and (v) updating the controls as part of a comprehensive continuous monitoring process.
- **Supporting appendices** provide more detailed security control selection and specification-related information including: (i) general references; (ii) definitions and terms; (iii) acronyms; (iv) baseline security controls for low-impact, moderate-impact, and high-impact information systems; (v) minimum assurance requirements; (vi) a master catalog of security controls; (vii) information security program management controls; (viii) international information security standards; and (ix) the application of security controls to industrial control systems.

CHAPTER TWO

THE FUNDAMENTALS

SECURITY CONTROL STRUCTURE, ORGANIZATION, BASELINES, AND ASSURANCE

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

2.1 SECURITY CONTROL ORGANIZATION AND STRUCTURE

Security controls described in this publication have a well-defined organization and structure. The controls are organized into seventeen *families*[20] for ease of use in the control selection and specification process. In addition, there are three general classes of security controls (i.e., management, operational, and technical). Each family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each control family. Table 1 summarizes the classes and families in the security control catalog and the associated family identifiers.

TABLE 1: SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS

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

To uniquely identify each security control, a numeric identifier is appended to the family identifier to indicate the number of the control within the control family. For example, CP-9 is the ninth control in the Contingency Planning family. The security control structure consists of three key components: (i) a *control* section; (ii) a *supplemental guidance* section; and (iii) a

[20] The seventeen security control families in NIST Special Publication 800-53, described in the security control catalog in Appendix F, are closely aligned with the seventeen security-related areas in FIPS 200 specifying the minimum security requirements for protecting federal information and information systems. One additional family provides controls for information security programs (Appendix G).

control enhancements section.[21] The following example from the Auditing and Accountability family illustrates the structure of a typical security control.

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

a. Alerts designated organizational officials in the event of an audit processing failure; and

b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

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

Control Enhancements:

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

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

(3) The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [*Selection: rejects or delays*] network traffic above those thresholds.

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

The control section provides a concise statement of the specific security capability needed to protect a particular aspect of an organization or information system. The control statement describes specific security-related activities or actions to be carried out by the organization or by the information system. For some controls in the control catalog, a degree of flexibility is provided by allowing organizations to selectively define input values for certain parameters associated with the controls. This flexibility is achieved through the use of *assignment* and *selection* operations within the main body of the control. Assignment and selection operations provide an opportunity for an organization to tailor the security controls to support specific mission, business, or operational needs. For example, an organization can specify the actions to be taken by the information system in the event of an audit processing failure (see AU-5 example above), the specific events to be audited within the system, the frequency of conducting system backups, restrictions on password use, or the distribution list for organizational policies and procedures. Once specified, the organization-defined values become 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 are expected to apply the supplemental guidance as appropriate, when defining, developing, and implementing security controls. In certain instances, the supplemental guidance provides more detail concerning the control requirements or important considerations and the needed flexibility for implementing security controls in the context of an organization's

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

operational environment, specific mission requirements, or assessment of risk. The supplemental guidance section also contains references to applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance documents (e.g., OMB Circulars, FIPS, and NIST Special Publications), and related controls.

The control enhancements section provides statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control. In both cases, the control enhancements are used in an information system requiring greater protection due to the potential impact of loss or when organizations seek additions to a basic control's functionality based on the results of a risk assessment. Control enhancements are numbered sequentially within each control so that the enhancements can be easily identified when selected to supplement the basic control. In the previous example for AU-5, if all three control enhancements are selected, the control designation subsequently becomes AU-5 (1) (2) (3). The numerical designation of a security control enhancement is used only to identify a particular enhancement within the control structure. The designation is neither indicative of the relative strength of the control enhancement nor assumes any hierarchical relationship among the enhancements. In the following example for CP-6, enhancement (3) is used before enhancement (2) since the third enhancement is required at a lower level than the second enhancement. This type of situation arises from the decision to maintain control stability in the face of change by not renumbering existing enhancements when new enhancements are added or when decisions about placement within baselines change.

CP-6 ALTERNATE STORAGE SITE

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

Supplemental Guidance: Related controls: CP-2, CP-9, MP-4.

Control Enhancements:

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

(2) **The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.**

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

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

2.2 SECURITY CONTROL BASELINES

Organizations are required to adequately mitigate the risk arising from use of information and information systems in the execution of missions and business functions. The challenge for organizations is to determine the appropriate set of security controls,[22] which if implemented and determined to be effective in their application, would most cost-effectively mitigate risk while complying with the specific security requirements defined by applicable laws, Executive Orders, directives, policies, standards, or regulations (e.g., Federal Information Security Management

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

Act, OMB Circular A-130, Appendix III). Selecting the appropriate set of security controls to adequately mitigate risk by meeting 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 organizational 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 starting point for the security control selection process described in this document and are determined by the information system security categorization in accordance with FIPS 199.[23] The tailored security control baseline (i.e., the appropriate control baseline from Appendix D adjusted in accordance with the guidance in Section 3.3) is the minimum set of security controls for the information system. Because the baselines are intended to be broadly applicable starting points, supplements to the tailored baselines (see Section 3.4) will likely be necessary in order to achieve adequate risk mitigation. The tailored baselines are supplemented based on organizational assessments of risk and the resulting controls documented in the security plans for the information systems.

Appendix D provides a listing of baseline security controls. Three sets of baseline controls have been identified corresponding to the low-impact, moderate-impact, and high-impact levels defined in the FIPS 199 security categorization process and used in Section 3.2 of this document to provide an initial set of security controls for each impact level.[24] Appendix F provides a catalog of security controls for information systems, arranged by control families. Chapter 3 provides additional information on how to use security categories to select the appropriate set of baseline security controls, how to apply the tailoring guidance to the baseline controls, and how to supplement the tailored baseline in order to achieve adequate risk mitigation.

Implementation Tip

There are additional security controls and control enhancements that appear in the security control catalog (Appendix F) that are found in only higher-impact baselines or not used in any of the baselines. These additional security controls and control enhancements for the information system are available to organizations and can be used in supplementing the tailored baselines to achieve the needed level of protection in accordance with an organizational assessment of risk. Moreover, security controls and control enhancements contained in higher-level baselines can also be used to strengthen the level of protection provided in lower-level baselines, if deemed appropriate. At the end of the security control selection process, the agreed-upon set of controls in the security plan must be sufficient to provide adequate security for the organization and mitigate risks to organizational operations and assets, individuals, other organizations, and the Nation.

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

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

2.3 COMMON CONTROLS

An organization-wide view of an information security program facilitates the identification of *common controls* that serve the protection needs of the organization at large. Common controls are security controls that are *inheritable* by one or more organizational information systems. The organization (typically the Office of the Chief Information Officer), assigns responsibility for organization-identified common controls to appropriate organizational officials and coordinates the implementation, assessment, and authorization/approval of the controls. The identification of common controls is most effectively accomplished as an organization-wide exercise with the involvement of authorizing officials, chief information officer, senior information security officer, information system owners, information owners/stewards, and information system security officers. The organization-wide exercise considers the categories of information systems within the organization in accordance with FIPS 199 (i.e., low-impact, moderate-impact, or high-impact) and the security controls necessary to adequately mitigate the risks arising from the use of those systems (see *baseline* security controls in Section 2.2). For example, common controls can be identified for all low-impact information systems by considering the baseline security controls for that category of information system. Similar exercises can be conducted for moderate-impact and high-impact systems as well.

Many of the security controls needed to protect organizational information systems (e.g., contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls) are excellent candidates for common control status. Information security program management controls (see Appendix G, PM family) may also be deemed common controls by the organization since the controls are employed at the organization level and serve all organizational information systems. By centrally managing and documenting the implementation, assessment, and authorization/approval of the common controls, 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 clearly identify which security controls have been designated by the organization as common controls and which controls have been designated as system-specific controls.

Common controls are documented in the organization-wide *information security program plan*.[25] Organizations have the flexibility to describe common controls in single or multiple documents. In the case of multiple documents, the documents describing the common controls are included as attachments to the information security program plan. If multiple documents are contained in the security program plan, the organization specifies in each document, the organizational official or officials responsible for the implementation, assessment, and approval/authorization of the common controls included in the respective documents. For example, the organization may require that the Facilities Management Office implement, assess, and approve/authorize common physical and environmental protection controls or that the Human Resources Office implement, assess, and approve/authorize common personnel security controls when such controls are not associated with an information system. When common controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems), the organization-wide information security program plan will indicate which separate security plans contain descriptions of the common controls.

[25] Information security program plans are described in Appendix G.

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 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 uses.

Information system owners are responsible for any system-specific issues associated with the implementation of an organization's common controls. These issues are identified and described in the security plans for the individual information systems. The senior information security officer, acting on behalf of the chief information officer, coordinates with common control providers (e.g., facilities managers, site managers, personnel managers) responsible for the implementation, assessment, and approval of the designated common controls to ensure that the required controls are put into place, the controls are assessed for effectiveness, and the assessment results are shared with the appropriate information system owners.

The common controls contained in the information security program plan are approved and/or authorized for use by a senior organizational official, with the same or similar authority and responsibility for managing risk as the authorization officials for information systems.[26] A plan of action and milestones document is developed and maintained for the common controls that are deemed through assessment, to be less than effective. Common controls are also subject to the same continuous monitoring requirements as security controls employed in individual organizational information systems.

The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Partitioning security controls into common controls and system-specific controls can result in significant savings to the organization in implementation and assessment costs. It can also result in a more consistent application of the security controls across the organization. While the concept of security control partitioning into common controls and system-specific controls is straightforward and intuitive, the application of this principle within an organization takes planning, coordination, and perseverance.

Implementation Tip

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

[26] In situations where common controls are inherited from external environments, organizations should consult the guidance provided in Section 2.4.

2.4 SECURITY CONTROLS IN EXTERNAL ENVIRONMENTS

Organizations are becoming increasingly reliant on information system services provided by external providers to carry out important missions and business functions. External information system services are services that are implemented outside of the authorization boundaries established by the organization. These external services may be used by, but are not part of, organizational information systems. In some situations, external information systems may completely replace the functionality of internal organizational systems.

Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. The growing dependence on external service providers and new relationships being forged with those providers present new and difficult challenges for the organization, especially in the area of information system security. These challenges include: (i) defining the types of external services provided to the organization; (ii) describing how the external services are protected in accordance with the security requirements of the organization; and (iii) obtaining the necessary assurances that the risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the use of the external services is acceptable.

The assurance or confidence that the risk from using external services is at an acceptable level depends on the trust[27] that the authorizing official places in the external service provider. In some cases, the level of trust is based on the amount of direct control the authorizing official is able to exert on the external service provider with regard to employment of security controls necessary for the protection of the service and the evidence brought forth as to the effectiveness of those controls. The level of control is usually established by the terms and conditions of the contract or service-level agreement with the external service provider and can range from extensive (e.g., negotiating a contract or agreement that specifies detailed security control requirements for the provider) to very limited (e.g., using a contract or service-level agreement to obtain commodity services[28] such as commercial telecommunications services). In other cases, the level of trust is based on factors that convince the authorizing official that the requisite security controls have been employed and that a credible determination of control effectiveness exists. For example, a separately authorized external information system service provided to an organization through a line of business relationship may provide a degree of trust in the external service within the tolerable risk range of the authorizing official.

The provision of services by providers external to the organization may result in some services without explicit agreements between the organization and the external entities responsible for the services. Whenever explicit agreements are feasible and practical (e.g., through contracts, service-level agreements, etc.), the organization should develop such agreements and require the use of the security controls in Special Publication 800-53. When the organization is not in a position to require explicit agreements with external service providers (e.g., the service is

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

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

imposed on the organization or the service is commodity service), the organization should establish explicit assumptions about the service capabilities with regard to security. Contracts between the organization and external service providers may also require the active participation of the organization. For example, the organization may be required by the contract to install public key encryption-enabled client software recommended by the service provider.

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

2.5 SECURITY CONTROL ASSURANCE

Assurance is the grounds for confidence[29] 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, implementers, and operators in the specification, design, development, implementation, operation, and maintenance of security controls;[30] and (ii) actions taken by security control assessors 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 (e.g., evaluators, auditors, information system owners, Inspectors General) are addressed in NIST Special Publication 800-53A.

Appendix E describes the minimum assurance requirements for security controls in low-impact, moderate-impact, and high-impact information systems. For security controls in low-impact systems, the emphasis is on the control being in place with the expectation that no obvious errors exist and that, as flaws are discovered, they are addressed in a timely manner. For security controls in moderate-impact systems, the emphasis is on increasing the grounds for confidence in control correctness. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer or control implementer incorporates, as part of the control, specific capabilities to increase grounds for confidence that the control meets its function or purpose. For

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

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

security controls in high-impact systems, the emphasis is on requiring within the control, the capabilities that are needed to support ongoing, consistent operation of the control and to support continuous improvement in the control's effectiveness. There are additional assurance requirements available to developers/implementers of security controls supplementing the minimum assurance requirements for the moderate-impact and high-impact information systems in order to protect against threats from highly skilled, highly motivated, and well-financed threat agents. This level of protection is necessary for those information systems where the organization is not willing to accept the risks associated with the type of threat agents cited above.

2.6 REVISIONS AND EXTENSIONS

The set of security controls listed in this publication represents the current state-of-the-practice safeguards and countermeasures for federal information systems and organizations. The controls will be carefully reviewed and revised periodically to reflect: (i) the experience gained from using the controls; (ii) changing security requirements; (iii) emerging threats and attack methods; (iv) current vulnerabilities; and (v) the availability of new security technologies.[31] The security controls in the security control catalog are expected to change over time, as controls are eliminated, revised and added. The security controls defined in the low, moderate, and high baselines are also expected to change over time as the level of security and due diligence for mitigating risks within organizations changes. In addition to the need for change, the need for stability will be addressed by requiring that proposed additions, deletions, or modifications to the catalog of security controls go through a rigorous public review process to obtain government and private sector feedback and to build consensus for the changes. A stable, yet flexible and technically rigorous set of security controls will be maintained in the security control catalog.

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

CHAPTER THREE

THE PROCESS

SELECTION AND SPECIFICATION OF SECURITY CONTROLS

This chapter describes the process of selecting and specifying security controls for an organizational information system to include: (i) using the *Risk Management Framework* to organize and guide the selection process; (ii) categorizing the information system in accordance with FIPS 199; (iii) selecting security controls, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based upon an organizational assessment of risk; and (iv) updating the controls as part of a comprehensive continuous monitoring process.

3.1 MANAGING RISK

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

- ***Categorize*** the information system and the information processed, stored, and transmitted by that system based on a FIPS 199 (worst case) impact analysis.
- ***Select*** an initial set of baseline security controls (Appendix D) for the information system based on the FIPS 199 security categorization and the minimum security requirements defined in FIPS 200; apply tailoring[32] guidance; supplement the tailored baseline security controls based on an assessment of risk[33] and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances; specify minimum assurance requirements (Appendix E).
- ***Implement*** the security controls in the information system and describe how the controls are employed with regard to specific hardware, software, or firmware components. For legacy systems, some or all of the security controls selected may already be in place.
- ***Assess*** the security controls in the information system using appropriate assessment 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.[34]

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

[33] NIST Special Publication 800-30 provides guidance on the assessment of risk.

[34] NIST Special Publication 800-53A provides guidance on assessing the effectiveness of security controls.

- ***Authorize*** information system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.[35]
- ***Monitor*** the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

Figure 1 illustrates the specific activities in the Risk Management Framework and the information security standards and guidance documents associated with each activity.[36] The remainder of this chapter focuses on several key activities in the Risk Management Framework associated with security control selection and specification.

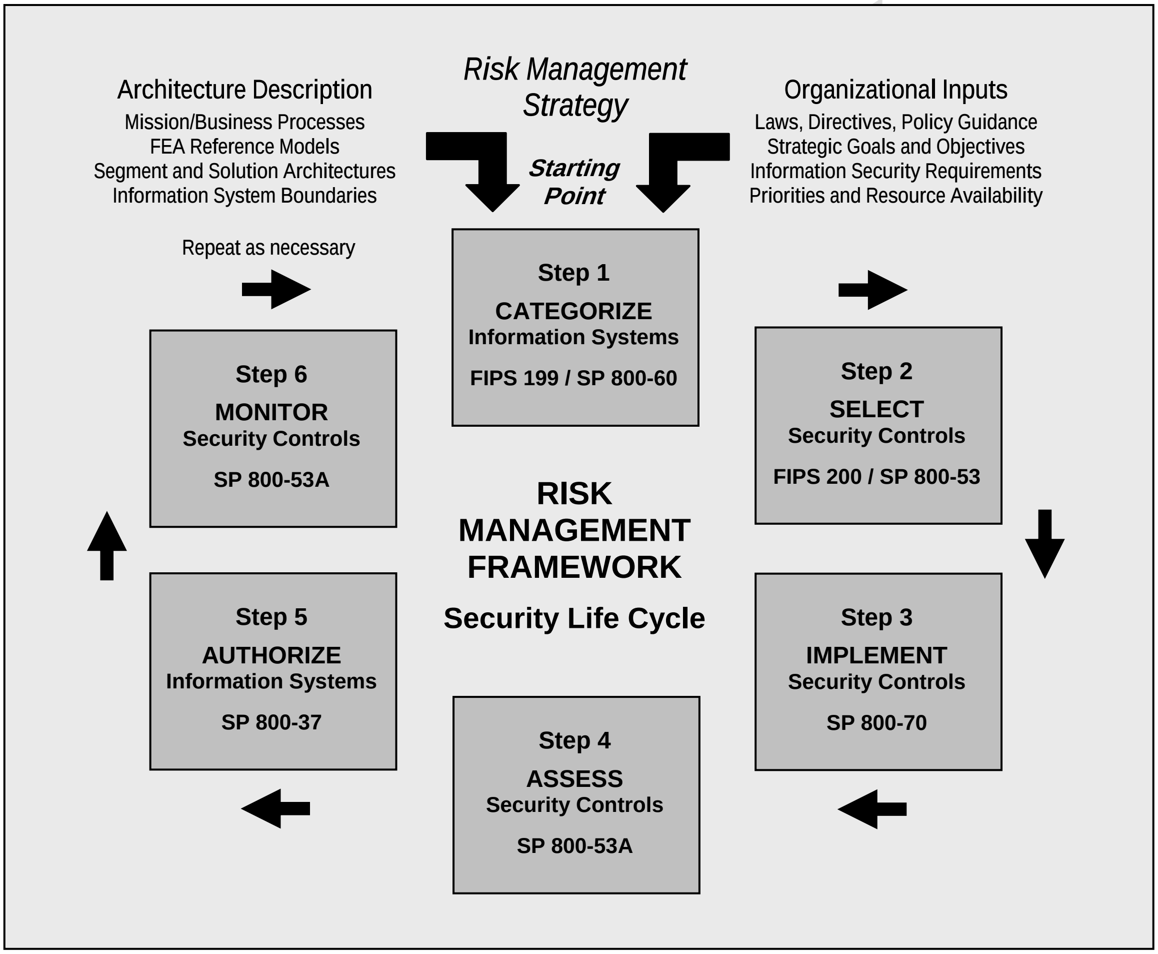

FIGURE 1: RISK MANAGEMENT FRAMEWORK

[35] NIST Special Publication 800-37 provides guidance on the security authorization of information systems.

[36] NIST Special Publication 800-39 further describes the RMF and provides guidance on organization-wide risk management including the development of risk management strategies, risk-related governance issues, defining protection requirements and associated risks for organizational mission/business processes, integration of security and privacy requirements into enterprise architectures, and managing risk within the system development life cycle.

3.2 CATEGORIZING THE INFORMATION SYSTEM

FIPS 199, the mandatory security categorization standard, is predicated on a simple and well-established concept—determining appropriate security priorities for organizational information systems and subsequently applying appropriate measures to adequately protect those systems. The security controls applied to a particular information system should be commensurate with the potential adverse impact on organizational operations, organizational assets, individuals, other organizations, and the Nation should there be a loss of confidentiality, integrity, or availability. FIPS 199 requires organizations to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability (RMF Step 1). 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 processed, stored, or transmitted by those information systems.[37] The generalized format for expressing the security category (SC) of an information system is:

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

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

Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept is used to determine the impact level of the information system for the express purpose of selecting an initial set of security controls from one of the three security control baselines.[38] 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.

Implementation Tip

To determine the overall impact level of the information system:

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

[37] 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.

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

3.3 SELECTING SECURITY CONTROLS

Once the overall impact level of the information system is determined based on the security categorization process, the organization begins the security control selection process (RMF Step 2). There are three steps in the control selection process carried out sequentially: (i) *selecting* the initial set of baseline security controls; (ii) *tailoring* the baseline security controls; and (iii) *supplementing* the tailored baseline. The following sections describe each of these steps in greater detail.

Selecting the Initial Baseline Security Controls

The first step in selecting security controls for the information system is to choose the appropriate set of baseline controls. The selection of the initial set of baseline security controls is based on the impact level of the information system and the information processed, stored, or transmitted by the system as determined by the security categorization process described in Section 3.2. The organization selects one of the three available sets of baseline security controls from Appendix D corresponding to the low-impact, moderate-impact, or high-impact rating of the information system.

Tailoring the Baseline Security Controls

After selecting the initial set of baseline security controls from Appendix D, the organization initiates the tailoring process to appropriately modify and more closely align the controls with the specific conditions within the organization (i.e., conditions specific to the information system or its environment of operation). The tailoring process includes several activities: (i) the application of *scoping guidance* to the initial baseline security controls; (ii) the specification of *compensating security controls*, if needed; and (iii) the specification of *organization-defined parameters* in the security controls, via explicit assignment and selection statements. To achieve a cost-effective, risk-based approach to providing adequate information security organization-wide, the baseline tailoring activities are coordinated with and approved by appropriate organizational officials (e.g., authorizing officials, authorizing officials' designated representatives, chief information officers, or senior information security officers). Tailoring decisions, including the specific rationale for those decisions, are documented in the security plan for the information system and approved by appropriate organizational officials as part of the security plan approval process.[39]

Scoping Guidance

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

- COMMON CONTROL-RELATED CONSIDERATIONS—

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

[39] This documentation is essential when examining the security considerations for information systems with respect to potential adverse impact on organizational operations and assets, individuals, other organizations, and the Nation.

- OPERATIONAL/ENVIRONMENTAL-RELATED CONSIDERATIONS—

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

- PHYSICAL INFRASTRUCTURE-RELATED CONSIDERATIONS—

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

- PUBLIC ACCESS-RELATED CONSIDERATIONS—

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

- TECHNOLOGY-RELATED CONSIDERATIONS—

  Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) are applicable only if those technologies are employed or are required to be employed within the information system.

  Security controls are applicable only to the components of the information system that provide or support the security capability addressed by the control and are sources of potential risk being mitigated by the control.[40] For example, when information system components are single-user, not networked, or part of a physically isolated network, one or more of these characteristics may provide appropriate rationale for not applying selected controls to that component.

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

Security controls that can be explicitly or implicitly supported by automated mechanisms, do not require the development of such mechanisms if the mechanisms do not already exist or are not readily available in commercial or government off-the-shelf products. If automated mechanisms are not readily available, cost-effective, or technically feasible, compensating security controls, implemented through nonautomated mechanisms or procedures, are used to satisfy specified security controls or control enhancements (see terms and conditions for applying compensating controls below).

- POLICY/REGULATORY-RELATED CONSIDERATIONS—

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

- SECURITY OBJECTIVE-RELATED CONSIDERATIONS—

  Security controls that uniquely support the confidentiality, integrity, or availability security objectives may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if not defined in a lower baseline) if, and only if, the downgrading action: (i) is consistent with the FIPS 199 security categorization for the corresponding security objectives of confidentiality, integrity, or availability before moving to the high water mark;[41] (ii) is supported by an organizational assessment of risk; and (iii) does not affect the security-relevant information within the information system.[42] The following security controls are recommended candidates for downgrading: (i) confidentiality [MA-3 (3), MP-2 (1), MP-3, MP-3 (1), MP-4, MP-5 (1) (2) (3), MP-6, PE-5, SC-4, SC-9]; (ii) integrity [SC-8]; and (iii) availability [CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, MA-6, PE-9, PE-10, PE-11, PE-13, PE-15, SC-6].[43]

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

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

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

Compensating Security Controls

With the diverse nature of today's information systems, organizations may find it necessary, on occasion, to specify and employ compensating security controls. A compensating security control is a management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provides equivalent or comparable protection for an information system and the information processed, stored, or transmitted by that system.[44] A compensating control for an information system may be employed by an organization only under the following conditions: (i) the organization selects the compensating control from NIST Special Publication 800-53, or if an appropriate compensating control is not available, the organization adopts a suitable compensating control from another source;[45] (ii) the organization provides supporting rationale for how the compensating control delivers an equivalent security capability for the information system and why the related baseline security control could not be employed; and (iii) the organization assesses and formally accepts the risk associated with employing the compensating control in the information system.

Organization-Defined Security Control Parameters

Security controls containing organization-defined parameters (i.e., assignment and/or selection operations) give organizations the flexibility to define certain portions of the controls to support specific organizational requirements or objectives (see AU-5 example in Section 2.1). After the application of scoping guidance and selection of compensating security controls, organizations review the list of security controls for assignment and selection operations and determine appropriate organization-defined values for the identified parameters. Where specified, minimum and maximum values for organization-defined parameters are adhered to unless more restrictive values are prescribed by applicable laws, Executive Orders, directives, policies, standards, or regulations or are indicated by the risk assessment in order to adequately mitigate risk.

Supplementing the Tailored Baseline

The tailored security control baseline should be viewed as the foundation or starting point in the selection of adequate security controls for an information system. The tailored baseline represents, for a particular class of information system (derived from the FIPS 199 security categorization and modified appropriately for conditions specific to the system or its environment of operation), the starting point for determining the needed level of security *due diligence* to be demonstrated by an organization toward the protection of its operations and assets. As described in Section 3.1, the final determination of the appropriate set of security controls necessary to provide adequate security for an information system is a function of the organization's assessment of risk and what is required to sufficiently mitigate the risks to organizational operations and assets, individuals, other organizations, and the Nation.[46]

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

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

[46] Considerations for potential national-level impacts and impacts to other organizations in categorizing organizational information systems derive from the USA PATRIOT Act and Homeland Security Presidential Directives.

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

There may be situations in which an organization is employing information technology beyond its ability to adequately protect critical and/or essential missions and business functions. That is, the organization cannot apply sufficient security controls within an information system to adequately reduce or mitigate risk. In those situations, an alternative strategy is needed to prevent the mission and business functions from being adversely affected; a strategy that considers the mission/business risks that result from an aggressive use of information technology. Information system use restrictions provide an alternative method to reduce or mitigate risk, for example, when: (i) security controls cannot be implemented within technology and resource constraints; or (ii) security controls lack reasonable expectation of effectiveness against identified threat sources. Restrictions on the use of information systems and specific information technologies are in many situations, the only practical or reasonable course of action an organization can take in order to have the ability to carry out its assigned missions and business functions in the face of determined adversaries.

Organizational officials having a vested interest in the accomplishment of the organization's missions and business functions determine the required system use restrictions. These officials typically include, for example, mission/business owners, information system owners, authorizing officials, senior information security officers, and chief information officers. Examples of use restrictions include: (i) limiting the information an information system can process, store, or transmit or the manner in which an organizational mission or business function is automated; (ii) prohibiting external access to organizational information by removing selected information system components from the network (i.e., air gapping); and (iii) prohibiting moderate- or high-impact information on an information system component to which the public has access, unless an explicit determination is made authorizing such access.

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

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

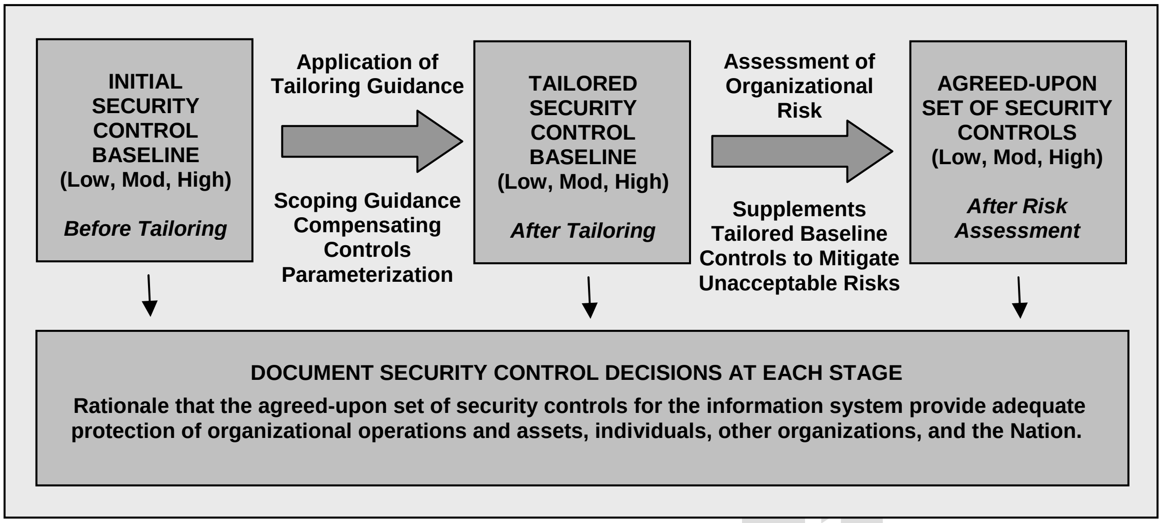
INITIAL SECURITY CONTROL BASELINE (Low, Mod, High)
Before Tailoring
Application of Tailoring Guidance
Scoping Guidance
Compensating Controls
Parameterization
TAILORED SECURITY CONTROL BASELINE (Low, Mod, High)
After Tailoring
Assessment of Organizational Risk
Supplements Tailored Baseline Controls to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

FIGURE 2: SECURITY CONTROL SELECTION PROCESS

3.4 MONITORING SECURITY CONTROLS

After the agreed upon set of security controls documented in the security plan are implemented, assessed for effectiveness, and the information system is authorized for operation in accordance with the organization's risk management strategy (RMF Steps 3, 4, and 5), the organization initiates specific actions as part of a comprehensive continuous monitoring program, including ongoing assessment of security control effectiveness, to determine if there is a need to modify/update the current, deployed set of security controls based on changes in the system or its environment of operation (RMF Step 6). In particular, the organization revisits the risk management activities described in the Risk Management Framework on a regular basis. Additionally, there are events which can trigger the immediate need to assess the security state of the information system and if required, modify/update the current security controls. These events include, for example:

- An incident results in a breach to the information system, producing a loss of confidence in the confidentiality, integrity, or availability of information processed, stored, or transmitted by the system;
- A newly identified, credible, information system-related threat to organizational operations and assets, individuals, other organizations, or the Nation is identified based on intelligence information, law enforcement information, or other credible sources of information; or
- Significant changes to the configuration of the information system through the removal or addition of new or upgraded hardware, software, or firmware or changes in the operational environment potentially degrade the security state of the system.

When such events occur, organizations should, at a minimum, take the following actions:[47]

[47] Organizations should determine the specific types of events that would trigger changes to the security controls within the information system and a resulting modification to the security plan. The decision to commit resources in light of such events should be guided by an organizational assessment of risk.

- *Reconfirm impact level of the information system and the information processed, stored, and/or transmitted by that system.*

  The organization reexamines the FIPS 199 impact level of the information system to confirm that the level previously established and approved by the authorizing official is still valid. The resulting analysis may provide new insights as to the overall importance of the information system in allowing the organization to fulfill its mission/business responsibilities.

- *Assess the current security state of the information system and the risk to organizational operations and assets, individuals, other organizations, and the Nation.*

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

- *Plan for and initiate any necessary corrective actions.*

  Based on the results of an updated risk assessment, the organization determines what additional security controls and/or control enhancements or corrective actions for existing controls are necessary to adequately mitigate risk.

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

- *Consider reauthorizing the information system.*

  Depending on the severity of the event, the adverse impact on organizational operations and assets, individuals, other organizations, and the Nation, and the extent of the corrective actions required to fix the identified weaknesses or deficiencies in the information system, the organization may need to consider reauthorizing the information system in accordance with the provisions of NIST Special Publication 800-37. The authorizing official makes the final determination on the need to reauthorize the information system in consultation with the system and mission/business owners, the senior information security officer, and the chief information officer. The authorizing official may choose to conduct a limited reauthorization focusing *only* on the affected components of the information system and the associated security controls and/or control enhancements which have been changed during the update. Authorizing officials have sufficient information available from security control assessments to initiate, with an appropriate degree of confidence, necessary corrective actions.

APPENDIX A

REFERENCES

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

LEGISLATION

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
3. Paperwork Reduction Act (P.L. 104-13), May 1995.
4. USA PATRIOT Act (P.L. 107-56), October 2001.
5. Privacy Act of 1974 (P.L. 93-579), December 1974.
6. Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, *Electronic Freedom of Information Act Amendments of 1996.*

POLICIES, DIRECTIVES, REGULATIONS, AND MEMORANDA

7. Code of Federal Regulations, Title 5, *Administrative Personnel*, Section 731.106, *Designation of Public Trust Positions and Investigative Requirements* (5 C.F.R. 731.106).
8. Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—Employees Responsible for the Management or Use of Federal Computer Systems, Section 930.301 through 930.305 (5 C.F.R 930.301-305).
9. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.
10. Office of Management and Budget, Federal Enterprise Architecture Program Management Office, *Business Reference Model* (v2.0), June 2003.
11. Office of Management and Budget Memorandum M-01-05, *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy*, December 2000.
12. Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001.
13. Office of Management and Budget Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, August 2003.
14. Office of Management and Budget Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 2003.
15. Office of Management and Budget Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 2003.
16. Office of Management and Budget Memorandum M-04-26, *Personal Use Policies and File Sharing Technology*, September 2004.
17. Office of Management and Budget Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*, February 2005.

18. Office of Management and Budget Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2005.

19. Office of Management and Budget Memorandum M-06-15, *Safeguarding Personally Identifiable Information,* May 2006.

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

21. Office of Management and Budget Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 2006.

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

23. Office of Management and Budget Memorandum, *Recommendations for Identity Theft Related Data Breach Notification Guidance*, September 2006.

24. Office of Management and Budget Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 2007.

25. Office of Management and Budget Memorandum M-08-09, *New FISMA Privacy Reporting Requirements for FY 2008*, January 2008.

26. Office of Management and Budget Memorandum M-08-21, *FY08 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 2008.

STANDARDS

27. International Organization for Standardization/International Electrotechnical Commission 27001, *Information Security Management System Requirements,* October 2005.

28. International Organization for Standardization/International Electrotechnical Commission 17799, *Code of Practice for Information Security Management,* June 2005.

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

    National Institute of Standards and Technology Federal Information Processing Standards Publication 140-3 (Draft), *Security Requirements for Cryptographic Modules*, July 2007.

30. National Institute of Standards and Technology Federal Information Processing Standards Publication 180-3, *Secure Hash Standard (SHS),* October 2008.

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

    National Institute of Standards and Technology Federal Information Processing Standards Publication 186-3 (Draft), *Digital Signature Standard (DSS),* November 2008.

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

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

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

35. National Institute of Standards and Technology Federal Information Processing Standards Publication 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*, July 2008.

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

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

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

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

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

GUIDELINES

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

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

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

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

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

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

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

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

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

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

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

52. 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.

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

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

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

56. National Institute of Standards and Technology Special Publication 800-28, Version 2, *Guidelines on Active Content and Mobile Code*, March 2008.

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

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

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

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

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

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

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

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

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

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

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

68. National Institute of Standards and Technology Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication,* November 2007.

69. National Institute of Standards and Technology Special Publication 800-39 (Second Public Draft), *Managing Risk from Information Systems: An Organizational Perspective*, April 2008.

70. National Institute of Standards and Technology Special Publication 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*, November 2005.

71. National Institute of Standards and Technology Special Publication 800-41, Revision 1 (Draft), *Guidelines on Firewalls and Firewall Policy*, July 2008.

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

73. National Institute of Standards and Technology Special Publication 800-44, Version 2, *Guidelines on Securing Public Web Servers*, September 2007.

74. National Institute of Standards and Technology Special Publication 800-45, Version 2, *Guidelines on Electronic Mail Security*, February 2007.

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

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

77. National Institute of Standards and Technology Special Publication 800-48, Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, July 2008.

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

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

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

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

82. National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, July 2008.

83. National Institute of Standards and Technology Special Publication 800-54, *Border Gateway Protocol Security*, July 2007.

84. National Institute of Standards and Technology Special Publication 800-55, Revision 1, *Performance Measurement Guide for Information Security*, July 2008.

85. National Institute of Standards and Technology Special Publication 800-56A (Revised), *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007.

86. National Institute of Standards and Technology Special Publication 800-57 (Revised), *Recommendation for Key Management*, March 2007.

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

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

89. National Institute of Standards and Technology Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.

90. National Institute of Standards and Technology Special Publication 800-61, Revision 1, *Computer Security Incident Handling Guide*, March 2008.

91. National Institute of Standards and Technology Special Publication 800-63-1 (Draft), *Electronic Authentication Guideline*, December 2008.

92. National Institute of Standards and Technology Special Publication 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, October 2008.

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

94. National Institute of Standards and Technology Special Publication 800-66, Revision 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, October 2008.

95. National Institute of Standards and Technology Special Publication 800-67, Version 1.1, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, May 2008.

96. National Institute of Standards and Technology Special Publication 800-68, Revision 1, *Guide to Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, October 2008.

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

98. National Institute of Standards and Technology Special Publication 800-70, Revision 1 (Draft), *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*, September 2008.

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

100. National Institute of Standards and Technology Special Publication 800-73-2, *Interfaces for Personal Identity Verification*, September 2008.

101. National Institute of Standards and Technology Special Publication 800-76-1, *Biometric Data Specification for Personal Identity Verification*, January 2007.

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

103. National Institute of Standards and Technology Special Publication 800-78-1, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, August 2007.

104. National Institute of Standards and Technology Special Publication 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*, June 2008.

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

106. National Institute of Standards and Technology Special Publication 800-82 (Final Public Draft), *Guide to Industrial Control Systems (ICS) Security*, September 2008.

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

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

109. National Institute of Standards and Technology Special Publication 800-85A, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73 Compliance)*, April 2006.

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

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

112. National Institute of Standards and Technology Special Publication 800-87, Revision 1, *Codes for the Identification of Federal and Federally-Assisted Organizations*, April 2008.

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

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

115. National Institute of Standards and Technology Special Publication 800-90 (Revised), *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, March 2007.

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

117. National Institute of Standards and Technology Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007.

118. National Institute of Standards and Technology Special Publication 800-95, *Guide to Secure Web Services*, August 2007.

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

120. National Institute of Standards and Technology Special Publication 800-97, *Establishing Robust Security Networks: A Guide to IEEE 802.11i*, February 2007.

121. National Institute of Standards and Technology Special Publication 800-98, *Guidance for Securing Radio Frequency Identification (RFID) Systems*, April 2007.

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

123. National Institute of Standards and Technology Special Publication 800-101, *Guidelines on Cell Phone Forensics*, May 2007.

124. National Institute of Standards and Technology Special Publication 800-103 (Draft), *An Ontology of Identity Credentials, Part I: Background and Formulation*, October 2006.

125. National Institute of Standards and Technology Special Publication 800-104, *A Scheme for PIV Visual Card Topography*, June 2007.

126. National Institute of Standards and Technology Special Publication 800-106 (Draft), *Randomized Hashing Digital Signatures*, August 2008.

127. National Institute of Standards and Technology Special Publication 800-107 (Draft), *Recommendation for Using Approved Hash Algorithms*, July 2008.

128. National Institute of Standards and Technology Special Publication 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions*, November 2008.

129. National Institute of Standards and Technology Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*, November 2007.

130. National Institute of Standards and Technology Special Publication 800-113, *Guide to SSL VPNs*, July 2008.

131. National Institute of Standards and Technology Special Publication 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*, November 2007.

132. National Institute of Standards and Technology Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*, September 2008.

133. National Institute of Standards and Technology Special Publication 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, November 2008.

134. National Institute of Standards and Technology Special Publication 800-121, *Guide to Bluetooth Security*, September 2008.

135. National Institute of Standards and Technology Special Publication 800-123, *Guide to General Server Security*, July 2008.

136. National Institute of Standards and Technology Special Publication 800-124, *Guidelines on Cell Phone and PDA Security*, October 2008.

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix B provides definitions for security terminology used within Special Publication 800-53. Unless specifically defined in this glossary, all terms used in this publication are consistent with the definitions contained in CNSS Instruction 4009, *National Information Assurance Glossary*.

Authorization
(to operate)

The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

Authorization Boundary

All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

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.

Attribute-Based Access Control

Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place.

Authentication
[FIPS 200]

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

Authenticity

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

Authorize Processing

See Authorization.

Authorizing Official

A senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

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

Ensuring timely and reliable access to and use of information.

Boundary Protection

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

Boundary Protection Device

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

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

Agency official responsible for:

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

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

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

Note: Organizations subordinate to federal agencies may use the term *Chief Information Officer* to denote individuals filling positions with similar security responsibilities to agency-level Chief Information Officers.

Commodity Service

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

Common Carrier

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

Common Control

A security control that is inherited by one or more organizational information systems.

Compensating Security Controls

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

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

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

Configuration Control
[CNSS Inst. 4009]

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

Countermeasures
[CNSS Inst. 4009]

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

Controlled Area

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

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

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

External Information System (or Component)

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

External Information System Service

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

External Information System Service Provider

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

Federal Enterprise Architecture
[FEA Program Management Office]

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

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

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

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

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

High-Impact System
[FIPS 200]

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

Incident
[FIPS 200]

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

Identity-Based Access Control

Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based upon user identity.

Industrial Control System

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

Information
[FIPS 199]

An instance of an information type.

Information Owner
[CNSS Inst. 4009]

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

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

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

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

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

Information Security 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]

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

[Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.]

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

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

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

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

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

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

Information Type
[FIPS 199]

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

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

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

Label

See Security Label.

Line of Business

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

Local Access

Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

Low-Impact System
[FIPS 200]
An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.

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

Malware
See Malicious Code.

Management Controls
[FIPS 200]
The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.

Marking
See Security Marking.

Media
[FIPS 200]
Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

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

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

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

Mobile Device
Portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain non-volatile memory) or portable computing and communications device with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones).

Moderate-Impact System
[FIPS 200]
An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high.

National Security Emergency Preparedness Telecommunications Services
[47 C.F.R., Part 64, App A]
Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States.

National Security Information

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

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

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

Network Access

Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

Non-repudiation

Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.

Object

Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object implies access to the information it contains.

Operational Controls
[FIPS 200]

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

Organization
[FIPS 200]

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

Organization-controlled Network

A telecommunications network where: (i) all the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology provides the same effect. Organization-controlled networking is typically organization-owned, yet may be organization-controlled while not being organization-owned.

Penetration Testing

A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.

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

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

Potential Impact
[FIPS 199]

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

Privacy Impact Assessment
[OMB Memorandum 03-22]

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

Privileged Account

An information system account with assigned authorizations of a privileged user.

Privileged Command

A human-initiated command executed on an information system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information.

Privileged User
[CNSS Inst. 4009, Adapted]

Individual who is authorized to enter one or more privileged commands.

Individual who has access to system control, monitoring, or administration functions often based on an assigned role (e.g., system administrator, information system security officer, maintainer, system programmer).

Protective Distribution System

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

Records

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

Remote Access

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

Remote Maintenance

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

Red Team Exercise

An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization.

Risk
[FIPS 200, Adapted]

The level of impact on organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system given the potential impact of identified threats and the likelihood of those threats occurring.

Risk Assessment

The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system.

Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

Risk Management
[FIPS 200, Adapted]

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

Role-based Access Control

Access control based on user roles (i.e., a collection of access authorizations a user receives based upon an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

Safeguards
[CNSS Inst. 4009, Adapted]

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

Scoping Guidance

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

Security Authorization (to operate)

See Authorization.

Security Authorization Boundary

See Authorization Boundary.

Security Category
[FIPS 199]

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

Security Controls
[FIPS 199]

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

Security Control Assessment

The testing and/or evaluation of the management, operational, and technical security controls in an 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.

Security Control Baseline
[FIPS 200]

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

Security Control Enhancements

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

Security Functions

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

Security Impact Analysis

The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.

Security Incident

See Incident.

Security Label

Explicit or implicit marking of a data structure providing access control or information flow control information.

Security Marking

Human-readable information affixed to information system components, removable media, or output indicating the distribution limitations, handling caveats and applicable security markings.

Security Objective
[FIPS 199]

Confidentiality, integrity, or availability.

Security Perimeter

See Authorization Boundary.

Security Plan

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

See System Security Plan or Security Program Plan.

Security Program Plan

Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.

Security-relevant Information

Any information within the information system that can potentially impact the operation of security functions in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data.

Security Requirements
[FIPS 200]

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

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

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

Note: Organizations subordinate to federal agencies may use the term *Senior Information Security Officer* or *Chief Information Security Officer* to denote individuals filling positions with similar security responsibilities to Senior Agency Information Security Officers.

Senior Information Security Officer

See Senior Agency Information Security Officer.

Spam

The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Spyware

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

Subsystem

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

System

See Information System.

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

A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.

System Security Plan
[NIST SP 800-18]

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

Tailoring

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

Tailored Security Control Baseline

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

Technical Controls
[FIPS 200]

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

Telecommunications Network

A collection of links and nodes arranged so that messages may be passed from one part of the network to another over multiple links and through various nodes. Messages are formatted according to a protocol that includes at least a destination address to which the message is delivered.

Threat
[CNSS Inst. 4009, Adapted]

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Threat Source
[FIPS 200]

The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.

Threat Assessment
[CNSS Inst. 4009]

Formal description and evaluation of threat to an information system.

Trusted Path

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

User
[CNSS Inst. 4009]

Individual or (system) process authorized to access an information system.

Vulnerability
[CNSS Inst. 4009, Adapted]

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Assessment
[CNSS Inst. 4009]

Formal description and evaluation of the vulnerabilities in an information system.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

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

APPENDIX D

SECURITY CONTROL BASELINES – SUMMARY

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

The following table lists the security control baselines that represent the starting point in determining the security controls for low-impact, moderate-impact, and high-impact information systems. The three security control baselines are hierarchical in nature with regard to the security controls employed in those baselines.[48] If a security control is selected for one of the baselines, the family identifier and control number are listed in the appropriate column. If a control is not used in a particular baseline, the entry is marked “not selected.” Control enhancements, when used to supplement basic security controls, are indicated by the number of the control enhancement. For example, an “IR-2 (1)” in the high baseline entry for the IR-2 security control indicates that the second control from the Incident Response family has been selected along with control enhancement (1). Some security controls and control enhancements in the security control catalog are not used in any of the baselines but are available for use by organizations if needed; for example, when the results of a risk assessment indicate the need for additional controls or control enhancements in order to adequately mitigate risks to individuals, the organization, or its assets. A complete description of security controls, supplemental guidance for the controls, and control enhancements is provided in Appendix F. A detailed listing of security controls and control enhancements for each control baseline is available at http://csrc.nist.gov/sec-cert.

[48] The hierarchical nature applies to the security requirements of each control (i.e., the base control plus all of its enhancements) at the low-impact, moderate-impact, and high-impact level in that the control requirements at a particular impact level (e.g., CP-4 *Contingency Plan Testing and Exercises*—Moderate: CP-4 (1)) meets a stronger set of security requirements for that control than the next lower impact level of the same control (e.g., CP-4 *Contingency Plan Testing and Exercises*—Low: CP-4).

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
Access Control				
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4) (5) (6)	AC-2 (1) (2) (3) (4) (5) (6)
AC-3	Access Enforcement	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6 (1) (2)	AC-6 (1) (2)
AC-7	Unsuccessful Login Attempts	AC-7	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8	AC-8
AC-9	Previous Logon Notification	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	Not Selected	Not Selected	AC-10
AC-11	Session Lock	Not Selected	AC-11	AC-11
AC-12	Session Termination (Withdrawn)	---	---	---
AC-13	Supervision and Review—Access Control (Withdrawn)	---	---	---
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking (Withdrawn)	---	---	---
AC-16	Automated Labeling	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	AC-17	AC-17 (1) (2) (3) (4) (5)	AC-17 (1) (2) (3) (4) (5) (6)
AC-18	Wireless Access Restrictions (Withdrawn)	---	---	---
AC-19	Access Control for Mobile Devices	AC-19	AC-19 (1) (2) (3)	AC-19 (1) (2) (3)
AC-20	Use of External Information Systems	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	User-Based Collaboration and Information Sharing	Not Selected	Not Selected	Not Selected
Awareness and Training				
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1
AT-2	Security Awareness	AT-2	AT-2	AT-2
AT-3	Security Training	AT-3	AT-3	AT-3
AT-4	Security Training Records	AT-4	AT-4	AT-4
AT-5	Contacts with Security Groups and Associations	Not Selected	Not Selected	Not Selected
Audit and Accountability				
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1
AU-2	Auditable Events	AU-2	AU-2 (3) (4)	AU-2 (3) (4)
AU-3	Content of Audit Records	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	Not Selected	AU-6	AU-6 (1)
AU-7	Audit Reduction and Report Generation	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	AU-8	AU-8 (1)	AU-8 (1)

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-9	Protection of Audit Information	AU-9	AU-9	AU-9
AU-10	Non-repudiation	Not Selected	Not Selected	Not Selected
AU-11	Audit Record Retention	AU-11	AU-11	AU-11
AU-12	Audit Generation	AU-12	AU-12	AU-12 (1)
Security Assessment and Authorization				
CA-1	Security Assessment and Authorization Policies and Procedures	CA-1	CA-1	CA-1
CA-2	Security Assessments	CA-2	CA-2 (1)	CA-2 (1)
CA-3	Information System Connections	CA-3	CA-3	CA-3
CA-4	Security Certification (Withdrawn)	---	---	---
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5
CA-6	Security Authorization	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7	CA-7	CA-7
Configuration Management				
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (1)	CM-2 (1) (2) (3) (4)
CM-3	Configuration Change Control	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	Not Selected	CM-4	CM-4
CM-5	Access Restrictions for Change	Not Selected	CM-5	CM-5 (1) (2) (3)
CM-6	Configuration Settings	CM-6	CM-6	CM-6 (1) (2)
CM-7	Least Functionality	Not Selected	CM-7 (1)	CM-7 (1) (2)
CM-8	Information System Component Inventory	CM-8	CM-8 (1)	CM-8 (1) (2) (3) (4)
CM-9	Configuration Management Plan	Not Selected	Not Selected	Not Selected
Contingency Planning				
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1)	CP-2 (1) (2) (3)
CP-3	Contingency Training	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing and Exercises	CP-4	CP-4 (1)	CP-4 (1) (2) (4)
CP-5	Contingency Plan Update (Withdrawn)	---	---	---
CP-6	Alternate Storage Site	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7 (1) (2) (3) (5)	CP-7 (1) (2) (3) (4) (5)
CP-8	Telecommunications Services	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1)	CP-9 (1) (2) (3)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10	CP-10 (3) (4)
Identification and Authentication				
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	IA-2	IA-2 (1)	IA-2 (1)
IA-3	Device Identification and Authentication	Not Selected	IA-3	IA-3

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

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-13	Fire Protection	PE-13	PE-13 (1) (2) (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	Not Selected	PE-18	PE-18 (1)
PE-19	Information Leakage	Not Selected	Not Selected	Not Selected
Planning				
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1
PL-2	System Security Plan	PL-2	PL-2	PL-2
PL-3	System Security Plan Update (Withdrawn)	---	---	---
PL-4	Rules of Behavior	PL-4	PL-4	PL-4
PL-5	Privacy Impact Assessment	PL-5	PL-5	PL-5
PL-6	Security-Related Activity Planning	Not Selected	PL-6	PL-6
Personnel Security				
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1
PS-2	Position Categorization	PS-2	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3	PS-3
PS-4	Personnel Termination	PS-4	PS-4	PS-4
PS-5	Personnel Transfer	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8
Risk Assessment				
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3
RA-4	Risk Assessment Update (Withdrawn)	---	---	---
RA-5	Vulnerability Scanning	RA-5	RA-5 (1)	RA-5 (1) (2) (3) (4) (5) (8)
System and Services Acquisition				
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2
SA-3	Life Cycle Support	SA-3	SA-3	SA-3
SA-4	Acquisitions	SA-4	SA-4 (1)	SA-4 (1)
SA-5	Information System Documentation	SA-5	SA-5 (1) (3)	SA-5 (1) (2) (3)
SA-6	Software Usage Restrictions	SA-6	SA-6	SA-6
SA-7	User Installed Software	SA-7	SA-7	SA-7
SA-8	Security Engineering Principles	Not Selected	SA-8	SA-8
SA-9	External Information System Services	SA-9	SA-9	SA-9
SA-10	Developer Configuration Management	Not Selected	Not Selected	SA-10

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-11	Developer Security Testing	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	Not Selected	Not Selected	SA-12
SA-13	Trustworthiness	Not Selected	Not Selected	SA-13
System and Communications Protection				
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1
SC-2	Application Partitioning	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	Not Selected	Not Selected	SC-3
SC-4	Information in Shared Resources	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5
SC-6	Resource Priority	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	SC-7	SC-7 (1) (2) (3) (4) (5) (10)	SC-7 (1) (2) (3) (4) (5) (6) (10) (11)
SC-8	Transmission Integrity	Not Selected	SC-8 (1)	SC-8 (1)
SC-9	Transmission Confidentiality	Not Selected	SC-9 (1)	SC-9 (1)
SC-10	Network Disconnect	Not Selected	SC-10	SC-10
SC-11	Trusted Path	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	Not Selected	SC-12	SC-12
SC-13	Use of Cryptography	SC-13	SC-13	SC-13
SC-14	Public Access Protections	SC-14	SC-14	SC-14
SC-15	Collaborative Computing Devices	Not Selected	SC-15	SC-15
SC-16	Transmission of Security Parameters	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17
SC-18	Mobile Code	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	SC-20 (1)	SC-20 (1)	SC-20 (1)
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	Not Selected	Not Selected	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	Not Selected	SC-22	SC-22
SC-23	Session Authenticity	Not Selected	SC-23	SC-23
SC-24	Fail in Known State	Not Selected	Not Selected	SC-24
SC-25	Thin Nodes	Not Selected	Not Selected	Not Selected
SC-26	Honeypots	Not Selected	Not Selected	Not Selected
SC-27	Operating System-Independent Applications	Not Selected	Not Selected	Not Selected
SC-28	Confidentiality of Information at Rest	Not Selected	SC-28	SC-28
SC-29	Heterogeneity	Not Selected	Not Selected	Not Selected
SC-30	Abstraction Techniques	Not Selected	Not Selected	Not Selected
SC-31	Covert Channel Analysis	Not Selected	Not Selected	Not Selected
System and Information Integrity				
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-2	Flaw Remediation	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	SI-3	SI-3 (1) (2) (3)	SI-3 (1) (2) (3)
SI-4	Information System Monitoring	Not Selected	SI-4 (2) (4) (5) (6)	SI-4 (2) (4) (5) (6)
SI-5	Security Alerts, Advisories, and Directives	SI-5	SI-5	SI-5 (1)
SI-6	Security Functionality Verification	Not Selected	Not Selected	SI-6
SI-7	Software and Information Integrity	Not Selected	Not Selected	SI-7 (1) (2)
SI-8	Spam Protection	Not Selected	SI-8	SI-8 (1)
SI-9	Information Input Restrictions	Not Selected	SI-9	SI-9
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	Not Selected	SI-10	SI-10
SI-11	Error Handling	Not Selected	SI-11	SI-11
SI-12	Information Output Handling and Retention	Not Selected	SI-12	SI-12
SI-13	Predictable Failure Prevention	Not Selected	Not Selected	Not Selected

APPENDIX E

MINIMUM ASSURANCE REQUIREMENTS

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

The minimum assurance requirements for security controls described in the security control catalog are listed below. The assurance requirements are directed at the activities and actions that security control developers and implementers[49] define and apply to increase the level of confidence that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. The assurance requirements are applied on a control-by-control basis. The requirements are grouped by information system impact level (i.e., low, moderate, and high) since the requirements apply to each control within the respective impact level. 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. Bolded text indicates requirements that appear for the first time at a particular impact level.

Low-impact Information Systems

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

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

Moderate-impact Information Systems

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

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

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

High-impact Information Systems

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

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

Additional Assurance Requirements for Moderate-impact and High-impact Information Systems

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

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

APPENDIX F

SECURITY CONTROL CATALOG

SECURITY CONTROLS, SUPPLEMENTAL GUIDANCE, AND CONTROL ENHANCEMENTS

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

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

The supplemental guidance section provides additional information related to a specific security control. Organizations are expected to apply the supplemental guidance as appropriate, when defining, developing, and implementing security controls. In certain instances, the supplemental guidance provides more detail concerning the control requirements or important considerations (and the needed flexibility) for implementing security controls in the context of an organization's operational environment, specific mission requirements, or assessment of risk. In addition, applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance documents (e.g., OMB Circulars, FIPS, and NIST Special Publications) are listed in the supplemental guidance section, when appropriate, for the particular security control.[50]

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

[50] NIST FIPS and Special Publications listed in the supplemental guidance sections of security controls refer to the most recent revisions to those publications.

Cautionary Notes

Security controls and control enhancements described in the security control catalog are employed in federal information systems in accordance with the risk management guidance provided in NIST Special Publication 800-39 as summarized in Chapter Three of this publication. This guidance includes the selection of minimum (baseline) security controls based upon the FIPS 199 security categorization of the information system and the tailoring of the baseline security controls by: (i) applying appropriate scoping guidance; (ii) specifying compensating controls, if needed; and (iii) inserting organization-defined security control parameters, where allowed. Security control parameters specified by organizations, must be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

The baseline security controls represent the minimum controls for low-impact, moderate-impact, and high-impact information systems, respectively. There are additional security controls and control enhancements that appear in the catalog that are not used in any of the baselines. These additional controls/enhancements are available to organizations and can be used in supplementing the tailored baselines to achieve the needed level of protection in accordance with an organizational assessment of risk. Moreover, security controls and control enhancements contained in higher-level baselines can also be used by organizations to strengthen the level of protection provided in lower-level baselines, if deemed appropriate.

Beginning with Revision 3 to NIST Special Publication 800-53, the supplemental guidance sections for security controls and control enhancements contain no control requirements. Therefore, NIST Special Publications listed in these sections, are *not* control requirements, but are provided as useful references. When compliance with a specific NIST publication *is* a control requirement, that requirement will be explicitly stated in the security control or control enhancement. Note that OMB policy mandating that all federal agencies operating other than national security systems comply with NIST Special Publications is not effected, being a separate requirement from the intent of the reference in supplemental guidance in this publication (see footnote 1, page iv, *Compliance with NIST Standards and Guidelines*).

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

a. A formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

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

Control Enhancements: None.

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

AC-2 ACCOUNT MANAGEMENT

Control: The organization manages information system accounts, including:

a. Identifying account types (i.e., individual, group, and system);.

b. Establishing conditions for group membership;

c. Identifying authorized users of the information system and specifying access rights/privileges;

d. Requiring appropriate approvals for requests to establish accounts;

e. Authorizing, establishing, activating, modifying, disabling, and removing accounts;

f. Reviewing accounts [*Assignment: organization-defined frequency*];

g. Specifically authorizing and monitoring the use of guest/anonymous accounts;

h. Notifying account managers when information system users are terminated; transferred, or information system usage or need-to-know/need-to-share changes; and

i. Granting access to the information system based on: (i) a valid need-to-know or need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage.

Supplemental Guidance: The identification of authorized users of the information system and the specification of access rights/privileges is consistent with the requirements in other security controls in the security plan. Related controls: AC-1, AC-3, AC-4, AC-5, AC-6, AC-10, AC-13, AC-17, AC-19, AC-20, AU-9, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SI-9, SC-13.

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 information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.

(5) The organization reviews currently active information system accounts [*Assignment: organization-defined frequency*] to verify that temporary accounts and accounts of terminated or transferred users have been deactivated in accordance with organizational policy.

(6) The organization prohibits the use of information system account identifiers as the identifiers for user electronic mail accounts.

LOW AC-2	**MOD** AC-2 (1) (2) (3) (4) (5) (6)	**HIGH** AC-2 (1) (2) (3) (4) (5) (6)

AC-3 ACCESS ENFORCEMENT

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

Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to enforcing authorized access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of an audited, manual override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant. Mechanisms implemented by AC-3 are configured to enforce authorizations determined by other security controls. Related controls: AC-1, AC-2, AC-4, AC-5, AC-6, AC-17, AC-19, AC-20, AU-9, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.

Control Enhancements:

(1) [Withdrawn: Incorporated into AC-6].

(2) The information system enforces dual authorization, based on organizational policies and procedures for [*Assignment: organization-defined privileged commands*].

Enhancement Supplemental Guidance: The organization does not employ dual authorization mechanisms when an immediate response is necessary to ensure public and environmental safety.

(3) The information system enforces one or more organization-defined nondiscretionary access control policies over [*Assignment: organization-defined set of users and resources*] where the policy rule set for each policy specifies:

(a) Access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day); and

(b) Required relationships among the access control information to permit access.

Enhancement Supplemental Guidance: Nondiscretionary access control policies that may be implemented by organizations include, for example, Attribute-Based Access Control, and Originator Controlled Access Control.

(4) The information system prevents access to [*Assignment: organization-defined security-relevant information*] except during secure, non-operable system states.

Enhancement Supplemental Guidance: Security relevant information is any information within the information system that can potentially impact the operation of security functions in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Secure, non-operable system states are states in which the information system is not performing mission/business-related processing (e.g., the system is off-line for maintenance, troubleshooting, boot-up, shutdown).

LOW AC-3	**MOD** AC-3	**HIGH** AC-3

AC-4 INFORMATION FLOW ENFORCEMENT

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

Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability. Mechanisms implemented by AC-4 are configured to enforce authorizations determined by other security controls. Related controls: AC-1, AC-17, AC-19, AC-21, AC-22, CM-7, PL-8, SA-8, SC-2, SC-5, SC-7, SC-18.

Control Enhancements:

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

Enhancement Supplemental Guidance: Information flow enforcement mechanisms compare labels on all information (data content and data structure) and respond appropriately (e.g., block, quarantine, alert administrator) when the mechanisms encounter information flows not explicitly allowed by the information flow policy. Information flow enforcement using explicit labels can be used, for example, to control the release of certain types of information.

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

(3) **The information system enforces dynamic information flow control allowing or disallowing information flows based upon changing conditions or operational considerations.**

(4) **The information system prevents encrypted data from bypassing content-checking mechanisms.**

(5) **The information system enforces [*Assignment: organization-defined limitations on the embedding of data types within other data types*].**

(6) **The information system enforces information flow control on metadata.**

(7) **The information system enforces [*Assignment: organization-defined one-way flows*] using hardware mechanisms.**

(8) **The information system enforces information flow control using [*Assignment: organization-defined security policy filters*] as a basis for flow control decisions.**

(9) **The information system enforces the use of human review for [*Assignment: organization-defined security policy filters*] when the system is not capable of making an information flow control decision.**

(10) **The information system provides the capability for a privileged administrator to enable/disable [*Assignment: organization-defined security policy filters*].**

(11) **The information system provides the capability for a privileged administrator to configure the [*Assignment: organization-defined security policy filters*] to support different security policies.**

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

AC-5 SEPARATION OF DUTIES

Control: The organization:

a. Establishes division of responsibilities and separates duties of individuals as necessary, to eliminate conflicts of interest; and

b. Implements separation of duties through assigned information system access authorizations.

Supplemental Guidance: Separation of duties prevents users from having the information system access necessary to perform malevolent 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. The access authorizations defined in this control are implemented by control AC-3. Related controls: AC-1, AC-3.

Control Enhancements: None.

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

AC-6 LEAST PRIVILEGE

Control: The organization employs the concept of least privilege, limiting authorized access for users (and processes acting on behalf of users) as necessary, to accomplish assigned tasks.

Supplemental Guidance: The access authorizations defined in this control are implemented by control AC-3. Related controls: AC-1, AC-3.

Control Enhancements:

(1) The organization explicitly authorizes access to [*Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information*].

Enhancement Supplemental Guidance: Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related control: AC-17.

(2) The organization requires that users of information system accounts with access to [*Assignment: organization-defined list of security functions or security-relevant information*], use non-privileged accounts when accessing other system functions, and if feasible, audits any use of privileged accounts for such functions.

(3) The organization authorizes network access to [*Assignment: organization-defined privileged commands*] only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

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

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

Control: The information system:

a. Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*] time period; and

b. Automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*], *delays next login prompt according to* [*Assignment: organization-defined delay algorithm.*]] when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance: Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization. If a delay algorithm is selected, the organization may chose to employ different algorithms for different information system components based upon the capabilities of those components. Response to unsuccessful login attempts may be implemented at both the operating system and the application level.

Control Enhancements:

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

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

AC-8 SYSTEM USE NOTIFICATION

Control: The information system:

a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording;

b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access, the information system; and

c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) ensures that any references to monitoring, recording, or auditing are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.

Supplemental Guidance: System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. System use notification is intended only for information system access that includes an interactive interface with a human user and is not intended to call for such an interface when the interface does not currently exist.

Control Enhancements: None.

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

AC-9 PREVIOUS LOGON NOTIFICATION

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

Supplemental Guidance: None.

Control Enhancements:

(1) The information system notifies the user, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon.

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

AC-10 CONCURRENT SESSION CONTROL

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

Supplemental Guidance: The organization may define the maximum number of concurrent sessions for an information system account globally, by account type, by account, or a combination. This control addresses concurrent sessions for a given information system account and does not address concurrent sessions by a single user via multiple system accounts.

Control Enhancements: None.

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

AC-11 SESSION LOCK

Control: The information system:

a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and

b. Retains the session lock until the user reestablishes access using appropriate identification and authentication procedures.

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

Control Enhancements:

(1) The information system session lock mechanism, when activated on a device with a display screen, places a publically viewable pattern onto the associated display, hiding what was previously visible on the screen.

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

AC-12 SESSION TERMINATION

[Withdrawn: Incorporated into SC-10].

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

[Withdrawn: Incorporated into AC-2 and AU-6].

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

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

Supplemental Guidance: The organization may allow limited user actions without identification and authentication (e.g., when individuals access public websites or other publicly accessible federal information systems such as the system at http://www.usa.gov). Organizations should also identify any actions that normally require identification or authentication but may, under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypass may be, for example, via a physical switch that is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not being repeated, but rather to situations where identification and/or authentication have not yet occurred. Related control: IA-2.

Control Enhancements:

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

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

AC-15 AUTOMATED MARKING

[Withdrawn: Incorporated into MP-3].

AC-16 AUTOMATED LABELING

Control: The information system labels information in storage, in process, and prior to transmission in accordance with:

a. Access control requirements;

b. Special dissemination, handling, or distribution instructions; or

c. Otherwise as required by the information system security policy.

Supplemental Guidance: Automated labeling refers to labels employed on internal data structures (e.g., records, buffers, files) within the information system. Such labels are often used to implement access control and flow control policies. Related controls: AC-1, AC-3, AC-4, SC-16.

Control Enhancements:

(1) The information system maintains the binding of the label to the information.

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

AC-17 REMOTE ACCESS

Control: The organization:

a. Documents allowed methods of remote access to the information system;

b. Establishes usage restrictions and implementation guidance for each allowed remote access method;

c. Authorizes remote access to the information system prior to connection; and

d. Enforces requirements for remote connections to the information system.

Supplemental Guidance: Remote access is any access to an organizational information system by a user (or process acting on behalf of a user) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Virtual Private Network (VPN) when adequately provisioned, may be treated as an organization-controlled network. With regard to wireless, radiated signals within organization-controlled facilities, typically qualify as outside organizational control. Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions to the information system associated with remote connections is accomplished by control AC-3. NIST Special Publication 800-77 provides guidance on IPsec-based virtual private networks. NIST Special Publications 800-48 and 800-97 provide guidance on wireless network security. NIST Special Publication 800-94 provides guidance on wireless intrusion detection and prevention. Related controls: AC-1, AC-3, AC-20, IA-2, IA-8.

Control Enhancements:

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

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

Enhancement Supplemental Guidance: The encryption strength of mechanism is selected based on the FIPS 199 impact level of the information. Related controls: SC-8, SC-9.

(3) The information system routes all remote accesses through a limited number of managed access control points.

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

Enhancement Supplemental Guidance: Related control: AC-6.

(5) The information system protects wireless access to the system using authentication and encryption.

Enhancement Supplemental Guidance: Authentication applies to user, device, or both as necessary.

(6) The organization monitors for unauthorized remote connections to the information system, including scanning for unauthorized wireless access points [*Assignment: organization-defined frequency*] and takes appropriate action if an unauthorized connection is discovered.

Enhancement Supplemental Guidance: Organizations proactively search for unauthorized remote connections including the conduct of thorough scans for unauthorized wireless access points. The scan is not necessarily limited to only those areas within the facility containing the information systems, yet is conducted outside of those areas only as needed to verify that unauthorized wireless access points are not connected to the system.

(7) The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issue.

(8) The organization does not allow users to independently configure wireless networking capabilities.

(9) The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.

(10) The organization ensures that remote sessions for accessing [*Assignment: organization-defined list of security functions and security-relevant information*] employ additional security measures [*Assignment: organization-defined security measures*] and are audited.

(11) The organization disables peer-to-peer wireless networking capability within the information system except for explicitly identified components in support of specific operational requirements.

(12) The organization disables Bluetooth wireless networking capability within the information system except for explicitly identified components in support of specific operational requirements.

LOW AC-17	**MOD** AC-17 (1) (2) (3) (4) (5)	**HIGH** AC-17 (1) (2) (3) (4) (5) (6)

AC-18 WIRELESS ACCESS RESTRICTIONS

[Withdrawn: Incorporated into AC-17].

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Control: The organization:

a. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices;

b. Authorizes connection of mobile devices to organizational information systems;

c. Monitors for unauthorized connections of mobile devices to organizational information systems;

d. Enforces requirements for the connection of mobile devices to organizational information systems;

e. Disables information system functionality that provides the capability for automatic execution of code on removable media without user direction;

f. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and

g. Applies specified measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.

Supplemental Guidance: Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Usage restrictions and implementation guidance related to mobile devices can include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Examples of information system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay.

Organizational policies and procedures for mobile devices used by individuals departing on and retuning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family. Related controls: MP-4, MP-5.

Control Enhancements:

(1) The organization restricts the use of writable, removable media in organizational information systems.

(2) The organization prohibits the use of personally-owned, removable media in organizational information systems.

(3) The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.

Enhancement Supplemental Guidance: An identifiable owner for removable media helps reduce the risk of employing such technology by assigning responsibility and accountability for addressing known vulnerabilities in the media (e.g., malicious code insertion).

LOW AC-19	**MOD** AC-19 (1) (2) (3)	**HIGH** AC-19 (1) (2) (3)

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

Control: The organization establishes terms and conditions for authorized individuals to:

a. Access the information system from an external information system; and

b. Process, store, and/or transmit organization-controlled information using an external information system.

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

Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system. This control does not apply to the use of external information systems to access public interfaces to organizational information systems and information (e.g., individuals accessing federal information through www.usa.gov). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system. This control defines access authorizations enforced by AC-3, rules of behavior requirements enforced by PL-4, and session establishment rules enforced by AC-17. Related controls: AC-1, AC-3, AC-17, PL-4.

Control Enhancements:

(1) The organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization:

(a) Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or

(b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system.

(2) The organization imposes restrictions on authorized individuals with regard to the use of organization-controlled removable media on external information systems.

LOW AC-20	**MOD** AC-20 (1) (2)	**HIGH** AC-20 (1) (2)

AC-21 USER-BASED COLLABORATION AND INFORMATION SHARING

Control: The organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [*Assignment: organization-defined information sharing circumstances where user discretion is required*].

Supplemental Guidance: Collaboration and information sharing is facilitated by manual processes or automated mechanisms to assist users in making information sharing/collaboration decisions. The control applies to information that may be restricted in some manner (e.g., privileged medical, contract-sensitive, proprietary, personally identifiable information). Depending on the information sharing circumstance, the sharing partner may be defined at the granularity of an individual, group, or organization; and information may be defined at the granularity of specific content, type, or security categorization.

Control Enhancements:

(1) The information system employs automated mechanisms to enable authorized users to make information sharing decisions based on access authorizations of sharing partners and access restrictions on information to be shared.

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

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

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

a. A formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

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

Control Enhancements: None.

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

AT-2 SECURITY AWARENESS

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

Supplemental Guidance: The organization determines the content of security awareness training and security awareness techniques based on the specific requirements of the organization and the information systems to which personnel have authorized access. Security awareness techniques can include, for example, displaying posters, offering security-messaged items, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events. The security awareness training program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301). NIST Special Publication 800-50 provides guidance on building security awareness training programs.

Control Enhancements:

(1) The organization includes practical exercises in security awareness training that simulate actual cyber attacks.

Enhancement Supplemental Guidance: Practical exercises may include, for example, no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking malicious web links.

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

AT-3 SECURITY TRAINING

Control: The organization:

a. Defines and documents information system security roles and responsibilities throughout the system development life cycle;

b. Identifies individuals having information system security roles and responsibilities; and

c. Provides security-related technical training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.

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

Control Enhancements: None.

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

AT-4 SECURITY TRAINING RECORDS

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

Supplemental Guidance: None.

Control Enhancements: None.

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

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

Control: The organization establishes and maintains contact with security groups and associations to stay up-to-date with the latest recommended security practices, techniques, and technologies and to share current security-related information including threats, vulnerabilities, and incidents.

Supplemental Guidance: Security groups and associations can include, for example, special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations, The groups and associations selected are consistent with the organization's mission/business requirements. Information sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Control Enhancements: None.

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

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

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

a. A formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

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

Control Enhancements: None.

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

AU-2 AUDITABLE EVENTS

Control: The organization:

a. Determines, based upon a risk assessment in conjunction with mission/business needs, which information system-related events require auditing [*Assignment: organization-defined list of auditable events and frequency of (or situation requiring) auditing for each identified auditable event*];

b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

c. Ensures that auditable events are adequate to support after-the-fact investigations of security incidents; and

d. Adjusts, as necessary, the events to be audited within the information system based on current threat information and ongoing assessments of risk.

Supplemental Guidance: The purpose of this control is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. NIST Special Publication 800-92 provides guidance on computer security log management. Related controls: AU-3, AU-13.

Control Enhancements:

(1) [Withdrawn: Incorporated into AU-13].

(2) [Withdrawn: Incorporated into AU-13].

(3) **The organization reviews and updates the list of organization-defined auditable events [*Assignment: organization-defined frequency*].**

(4) **The organization includes execution of privileged functions in the list of events to be audited by the information system.**

LOW AU-2	**MOD** AU-2 (3) (4)	**HIGH** AU-2 (3) (4)

AU-3 CONTENT OF AUDIT RECORDS

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

Supplemental Guidance: Audit record content includes, for example: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event. Related controls: AU-2, AU-8.

Control Enhancements:

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

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

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

AU-4 AUDIT STORAGE CAPACITY

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

Supplemental Guidance: The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Related controls: AU-2, AU-5, AU-6, AU-7.

Control Enhancements: None.

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

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

a. Alerts designated organizational officials in the event of an audit processing failure; and

b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

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

Control Enhancements:

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

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

(3) The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [*Selection: rejects or delays*] network traffic above those thresholds.

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

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

Control: The organization:

a. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and

b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

Supplemental Guidance: Related control: AU-7.

Control Enhancements:

(1) The information system employs automated mechanisms to integrate audit review, analysis, and reporting into organizational processes for investigation and response to suspicious activities.

(2) [Withdrawn: Incorporated into SI-4].

(3) The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

(4) The information system employs automated mechanisms to centralize audit review and analysis of audit records from multiple components within the system.

Enhancement Supplemental Guidance: An example of an automated mechanism for centralized review and analysis is a Security Information Management (SIM) product. Related control: AU-2.

(5) The organization integrates analysis of audit records with analysis of performance and network monitoring information to further enhance the ability to identify inappropriate or unusual activity.

Enhancement Supplemental Guidance: Related control: AU-7.

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

AU-7 AUDIT REDUCTION AND REPORT GENERATION

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

Supplemental Guidance: An audit reduction, review, and reporting capability provides support for near real-time audit review, analysis, and reporting requirements described in AU-6 and after-the-fact investigations of security incidents. Audit reduction and reporting tools do not alter original audit records. Related control: AU-6.

Control Enhancements:

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

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

AU-8 TIME STAMPS

Control: The information system uses internal system clocks to generate time stamps for audit records.

Supplemental Guidance: Time stamps generated by the information system include both date and time. Related control: AU-3.

Control Enhancements:

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

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

AU-9 PROTECTION OF AUDIT INFORMATION

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

Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. Related controls: AC-3, AC-6.

Control Enhancements:

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

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

AU-10 NON-REPUDIATION

Control: The information system protects against an individual falsely denying having performed a particular action.

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

Control Enhancements: None.

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

AU-11 AUDIT RECORD RETENTION

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

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

Control Enhancements: None.

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

AU-12 AUDIT GENERATION

Control: The information system:

a. Provides audit record generation capability for the auditable events defined in AU-2;

b. Provides audit record generation capability at [*Assignment: organization-defined information system components*]; and

c. Allows authorized users to select which auditable events are to be audited by specific components of the system;

d. Generates audit records for the selected list of auditable events defined in AU-2.

Supplemental Guidance: Audits records can be generated from various components within the information system. This control defines the specific information system components providing auditing capability. Related controls: AU-2, AU-3.

Control Enhancements: None.

(1) The information system provides the capability to compile audit records from multiple components within the system into a system-wide (logical or physical) audit trail that is time-correlated to within [*Assignment: Organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail*].

Enhancement Supplemental Guidance: This control does not require that audit records from every component that provides auditing capability within the information system be included in the system-wide audit trail. The audit trail is time-correlated if the time stamp in the individual audit records can be reliably related to the time stamp in other audit records to achieve a time ordering of the records within the organization-defined tolerance.

LOW AU-12	**MOD** AU-12	**HIGH** AU-12 (1)

FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION **CLASS:** MANAGEMENT

CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

a. Formal, documented, security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated assessment and authorization controls.

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

Control Enhancements: None.

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

CA-2 SECURITY ASSESSMENTS

Control: The organization:

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

b. Produces a security assessment report that documents the results of the assessment.

Supplemental Guidance: The organization assesses the security controls in an information system as part of: (i) security authorization or reauthorization; (ii) meeting the FISMA requirement for annual assessments; (iii) continuous monitoring; and (iv) testing/evaluation of the information system as part of the system development life cycle process. The FISMA requirement for (at least) annual security control assessments should *not* be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security authorization process. To satisfy the annual FISMA assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) security assessments conducted as part of an information system authorization or reauthorization process; (ii) continuous monitoring (see CA-7); or (iii) testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed.

Subsequent to the initial authorization of the information system and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring. The selection of an appropriate subset of security controls for the information system is based on: (i) the FIPS 199 security categorization of the system; (ii) the specific security controls selected and employed by the organization; and (iii) the level of assurance that the organization must have in determining the effectiveness of the security controls. The organization establishes the selection criteria and subsequently selects a subset of the security controls employed within the information system for assessment. Those security controls that are volatile/critical to protecting the information system are assessed at least annually. All other controls are assessed at least once during the information system's three-year authorization cycle. The organization can use the current year's assessment results from any of the above sources to meet the annual FISMA assessment requirement provided that the results are current, valid, and relevant to determining security control effectiveness. NIST Special Publication 800-53A provides guidance on security control assessments to include reuse of existing assessment results. External audits (e.g., audits conducted by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-6, CA-7, SA-11.

Control Enhancements:

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

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

(2) The organization includes as part of security control assessments, periodic, unannounced, in-depth monitoring, penetration testing, and red team exercises.

Enhancement Supplemental Guidance: A standard method for penetration testing consists of: (i) pre-test analysis based on full knowledge of the target system; (ii) pre-test identification of potential vulnerabilities based on pre-test analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. Detailed rules of engagement are agreed upon by all parties before the commencement of any penetration testing scenario. An organizational assessment of risk guides the decision on the level of independence required for penetration agents or penetration teams conducting penetration testing. Red team exercises are conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization. While penetration testing may be laboratory-based testing, red team exercises are intended to be more comprehensive in nature and reflect real-world conditions. Information system monitoring, penetration testing, and red-team exercises are conducted to improve the readiness of the organization by exercising organizational capabilities and indicating current performance levels as a means of focusing organizational actions to improve the security state of the system and organization. NIST Special Publication 800-53A provides guidance on penetration testing.

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

CA-3 INFORMATION SYSTEM CONNECTIONS

Control: The organization:

a. Authorizes all connections from the information system to other information systems outside of the authorization boundary through the use of system connection agreements;

b. Documents the information system connections and associated security requirements for each connection; and

c. Monitors the information system connections on an ongoing basis verifying enforcement of documented security requirements.

Supplemental Guidance: Since FIPS 199 security categorizations apply to individual information systems, the organization carefully considers the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Each interconnection between information systems must be addressed individually, documenting the interface characteristics. The level of formality for this documentation varies depending upon the relationship between the information systems. The relationship ranges from information systems with the same owner for which there is no need of an agreement but simply a description of the interface characteristics, to systems within different cabinet-level agencies necessitating a formal Interconnection Security Agreement (ISA) and a Memorandum of Understanding/Agreement (MOU/A). In every case, documenting the interface characteristics is required, yet the formality and approval process vary considerably even though all accomplish the same fundamental objective of managing the risk being incurred by the interconnection of the information systems. Risk considerations also include information systems sharing the same networks. NIST Special Publication 800-47 provides guidance on connecting information systems. Related controls: SC-7, SA-9.

Control Enhancements: None.

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

CA-4 SECURITY CERTIFICATION

[Withdrawn: Incorporated into CA-2].

CA-5 PLAN OF ACTION AND MILESTONES

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

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

Control Enhancements: None.

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

CA-6 SECURITY AUTHORIZATION

Control: The organization:

a. Assigns a senior-level executive or manager to the role of authorizing official for the information system;

b. Authorizes the information system for processing before commencing operations; and

c. Updates the security authorization [*Assignment: organization-defined frequency, at least every three years*] or when there is a significant change to the system.

Supplemental Guidance: OMB Circular A-130, Appendix III, establishes policy for security authorizations of federal information systems. Authorizing officials are senior officials or executives with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations and assets, individuals, other organizations, and the Nation. Authorizing officials typically have budgetary oversight for information systems or are responsible for the mission or business operations supported by the systems. Security authorization is an inherently federal responsibility and therefore, authorizing officials must be federal employees. Through the security authorization process, authorizing officials are accountable for the security risks associated with information system operations. Accordingly, authorizing officials should be in management positions with a level of authority commensurate with understanding and accepting such information system-related security risks. Through the employment of a comprehensive continuous monitoring process, the critical information contained in the authorization package (i.e., the security plan (including risk assessment), the security assessment report, and the plan of action and milestones) is updated on an ongoing basis providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system. To reduce the administrative burden of the three-year reauthorization process, the authorizing official uses the results of the continuous monitoring process to the maximum extent possible as the basis for rendering a reauthorization decision. NIST Special Publication 800-37 provides guidance on the security authorization of information systems. Related controls: CA-2, CA-7.

Control Enhancements: None.

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

CA-7 CONTINUOUS MONITORING

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

Supplemental Guidance: A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management for information systems. An effective continuous monitoring program includes: (i) configuration management and control of information system components; (ii) security impact analyses of changes to the system or its environment of operation; (iii) ongoing assessment of security controls; and (iv) status reporting..

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

Control Enhancements:

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

Enhancement Supplemental Guidance: The organization can extend and maximize the value of the ongoing assessment of security controls during the continuous monitoring process by requiring an independent assessor or team to assess all of the security controls during the information system's three-year authorization cycle. See supplemental guidance for CA-2, enhancement (1) for further information on assessor independence. Related controls: CA-2, CA-5, CA-6, CM-4.

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

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

a. A formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

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

Control Enhancements: None.

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

CM-2 BASELINE CONFIGURATION

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

Supplemental Guidance: This control establishes a baseline configuration for the information system and its constituent components including communications and connectivity-related aspects of the system. The baseline configuration provides information about the components of an information system and each component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. The baseline configuration is a well-defined, documented, and up-to-date specification to which the information system is built. Maintaining the baseline configuration involves creating new baselines as the information system changes over time, and keeping old baselines available for possible rollback. The baseline configuration of the information system is consistent with the organization's enterprise architecture. Related controls: CM-6, CM-8.

Control Enhancements:

(1) The organization reviews and updates the baseline configuration of the information system:

(a) [*Assignment: organization-defined frequency*];

(b) When required due to [*Assignment organization-defined circumstances*]; and

(c) As an integral part of information system component installations and upgrades.

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

(3) The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.

(4) The organization employs a deny-all, permit-by-exception authorization policy to identify software allowed on organizational information systems (i.e., white lists of authorized software).

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

CM-3 CONFIGURATION CHANGE CONTROL

Control: The organization:

a. Authorizes and documents changes to the information system;

b. Retains and reviews records of configuration-managed changes to the system; and

c. Audits activities associated with configuration-managed changes to the system.

Supplemental Guidance: Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control includes changes to components of the information system, changes to the configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers), emergency changes, and changes to remediate flaws. Approvals to implement changes to the information system consider the results from security impact analyses. Organizations consider including an information security representative (e.g., information system security officer, information system security manager) in the configuration change control process. An organizationally-approved process for managing configuration changes to the information system includes, for example, a chartered Configuration Control Board). Related controls: CM-4, CM-5, CM-6, SI-2.

Control Enhancements:

(1) The organization employs automated mechanisms to:

(a) Document proposed changes to the information system;

(b) Notify designated approval authorities;

(c) Highlight approvals that have not been received by [*Assignment: organization-defined time period*];

(d) Inhibit change until designated approvals are received; and

(e) Document completed changes to the information system.

(2) The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

Enhancement Supplemental Guidance: The organization ensures that testing does not interfere with information system functions. The individual/group conducting the tests understands the organizational information security policies and procedures, the information system security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. A production information system may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If an information system must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. In situations where the organization cannot, for operational reasons, conduct live testing of a production system, the organization employs compensating controls (e.g., providing a replicated system to conduct testing) in accordance with the general tailoring guidance.

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

CM-4 SECURITY IMPACT ANALYSIS

Control: The organization analyzes changes to the information system prior to implementation and as part of the change approval process to determine to potential effects of the changes on the security state of the system.

Supplemental Guidance: Security impact analysis may include for example, reviewing information system documentation such as the security plan to understand how specific security controls are implemented within the system and how the changes might affect the controls. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional safeguards and countermeasures are required. After the information system is changed (including system upgrades and modifications), the organization checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system (see CA-2). Security impact analysis is an important activity in the ongoing monitoring of security controls in the information system. Related controls: CA-2, CA-7, CM-3.

Control Enhancements: None.

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

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control: The organization:

a. Defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system; and

b. Generates, retains, and reviews [*Assignment: organization-defined frequency*] records reflecting all such changes.

Supplemental Guidance: Any changes to the hardware, software, and/or firmware components of the information system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications. Additionally, maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after the fact actions should the organization become aware of an unauthorized change to the information system. Access restrictions for change also include software libraries. Examples of access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes are implemented into a third-party interface rather than directly into the information system component), and change windows (e.g., changes occur only during specified times making unauthorized changes outside the window, easy to discover). Some or all of the enforcement mechanisms and processes necessary to implement this security control are included in other controls. For measures implemented in other controls, this control provides information to be used in the implementation of the other controls to cover specific needs related to enforcing authorizations to make changes to the information system, auditing changes, and retaining and review records of changes. Related controls: AC-3, AC-6, PE-3.

Control Enhancements:

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

(2) The organization conducts audits of information system changes at [*Assignment: organization-defined frequency*] and when indications so warrant to determine whether unauthorized changes have occurred.

(3) The information system prevents the installation of device drivers that are not signed with an organizationally recognized and approved certificate.

LOW Not Selected	**MOD** CM-5	**HIGH** CM-5 (1) (2) (3)

CM-6 CONFIGURATION SETTINGS

Control: The organization:

a. Establishes and documents mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements;

b. Implements the configuration settings;

c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based upon explicit operational requirements;

d. Enforces the configuration settings in all components of the information system; and

e. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Supplemental Guidance: Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Security-related parameters are those parameters impacting the security state of the system including parameters related to meeting other security control requirements. Security-related parameters include for example, registry settings; account, file, and directory settings (i.e., permissions); and settings for services, ports, and remote connections. Organizations consider establishing organization-wide mandatory configuration settings from which the settings for a given information system are derived. The Security Content Automation Protocol (SCAP) and defined standards within the protocol (e.g., Common Configuration Enumeration), provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy and provides guidance on configuration requirements for federal information systems (e.g., Federal Desktop Core Configuration). There are many security controls potentially affected by the mandatory requirements in the Federal Desktop Core Configuration (e.g., AC-19, CM-7). NIST Special Publication 800-70 provides guidance on producing and using configuration settings for information technology products employed in organizational information systems. Related controls: CM-2, CM-3, SI-4.

Control Enhancements:

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

(2) **The organization employs automated mechanisms to respond to unauthorized changes to [*Assignment: organization-defined configuration settings*].**

Enhancement Supplemental Guidance: Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring mandatory/organization-defined configuration settings, or in the extreme case, halting affected information system processing.

(3) **The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.**

Enhancement Supplemental Guidance: Related controls: IR-4, IR-5.

LOW CM-6	**MOD** CM-6	**HIGH** CM-6 (1) (2)

CM-7 LEAST FUNCTIONALITY

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

Supplemental Guidance: Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by organizational information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing). Organizations consider disabling unused or unnecessary physical and logical ports and protocols (e.g., universal serial bus [USB], PS/2, FTP) on information system components to prevent unauthorized connection of devices (e.g., USB drives). Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host intrusion detection systems to identify and prevent the use of prohibited ports, protocols, and services. Related control: RA-5.

Control Enhancements:

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

(2) The organization employs automated mechanisms to prevent program execution in accordance with [*Selection (one or more): organization-defined white-lists, black-lists, gray-lists*].

Enhancement Supplemental Guidance: A white-list is an organization-defined list of authorized software programs; a black-list is an organization-defined list of unauthorized software programs; and a gray-list is an organization-defined list of rules for authorizing execution of software programs, for example, by user or time-of-day with either allowed (white) or disallowed (black) results.

LOW Not Selected	**MOD** CM-7 (1)	**HIGH** CM-7 (1) (2)

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Control: The organization develops, documents, and maintains an inventory of the components of the information system that:

a. Accurately reflects the current information system;

b. Is consistent with the authorization boundary of the information system;

c. Is at the level of granularity deemed necessary for tracking and reporting; and

d. Includes [*Assignment: organization-defined information deemed necessary to achieve effective property accountability*].

Supplemental Guidance: Information deemed to be necessary by the organization to achieve effective property accountability can include, for example, manufacturer, model number, serial number, software license information, information system/component owner, and for a networked component/device, the machine name and network address. Related controls: CM-2, CM-6.

Control Enhancements:

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

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

Enhancement Supplemental Guidance: Organizations maintain the information system inventory to the extent feasible. Virtual machines, for example, can be difficult to monitor because they are not visible to the network when not in use. In such cases, the intent of this enhancement is to maintain as up-to-date, complete, and accurate an inventory as is reasonable.

(3) The organization:

(a) Employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the addition of unauthorized components/devices into the information system; and

(b) Disables network access by such components/devices or notifies designated organizational officials.

Enhancement Supplemental Guidance: This enhancement is in addition to the monitoring for unauthorized remote connections in AC-17 and for unauthorized mobile devices in AC-19. The monitoring for unauthorized components/devices on information system networks may be accomplished on an ongoing basis or by the periodic scanning of the networks for that purpose. Related controls: AC-17, AC-19.

(4) The organization includes in property accountability information for information system components, the names of the individuals responsible for administering those components.

LOW CM-8	**MOD** CM-8 (1)	**HIGH** CM-8 (1) (2) (3) (4)

CM-9 CONFIGURATION MANAGEMENT PLAN

Control: The organization develops and implements a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Defines the configuration items for the information system;

c. Defines when (in the system development life cycle) the configuration items are placed under configuration management;

d. Defines the means for uniquely identifying configuration items throughout the system development life cycle; and

e. Defines the process for managing the configuration of the configuration items.

Supplemental Guidance: Configuration Items are the information system items (hardware, software, firmware, and documentation) to be configuration managed. The configuration management plan satisfies the requirements in the organization’s configuration management policy while being tailored to the individual information system. The configuration management plan defines detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. It includes the steps for moving a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how development, test, and operational environments are controlled, and how documents are developed, released, and updated. Related control: SA-10.

Control Enhancements: None.

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

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

a. A formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

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

Control Enhancements: None.

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

CP-2 CONTINGENCY PLAN

Control: The organization:

a. Develops a contingency plan for the information system that:

- Identifies essential mission and business functions and associated contingency requirements;
- Provides restoration priorities and metrics;
- Addresses contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption, compromise, or failure; and
- Is reviewed and approved by designated officials within the organization;

b. Distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel and organizational elements*]; and

c. Coordinates contingency planning activities with incident handling activities;

d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*];

e. Revises the contingency plan to address system/organizational changes or problems encountered during contingency plan implementation, execution, or testing; and

f. Communicates contingency plan changes to [*Assignment: organization-defined list of key contingency personnel and organizational elements*].

Supplemental Guidance: Full range contingency planning addresses continuity of mission/business operations to include both information system restoration and implementation of alternative mission/business processes when systems are compromised. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission/business effectiveness, such as malicious attacks compromising the confidentiality or integrity of the information system. Examples of actions to call out in contingency plans include, for example, graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, or operating in a mode that is reserved solely for when the system is under attack. Related controls: CP-6, CP-7, CP-8, IR-4.

Control Enhancements:

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

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

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

(3) The organization identifies circumstances that can inhibit recovery and reconstitution of the information system to a known, secure state and provides compensating controls to mitigate risk.

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

CP-3 CONTINGENCY TRAINING

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

Supplemental Guidance: None.

Control Enhancements:

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

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

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

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

Control: The organization:

a. Tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan; and

b. Reviews the contingency plan test/exercise results and initiates corrective actions.

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

Control Enhancements:

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

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

(2) The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

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

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

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

CP-5 CONTINGENCY PLAN UPDATE

[Withdrawn: Incorporated into CP-2].

CP-6 ALTERNATE STORAGE SITE

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

Supplemental Guidance: Related controls: CP-2, CP-9, MP-4.

Control Enhancements:

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

(2) **The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.**

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

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

CP-7 ALTERNATE PROCESSING SITE

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

Supplemental Guidance: Equipment and supplies required to resume operations within the organization-defined time period are either available at the alternate site or contracts are in place to support delivery to the site. Timeframes to resume information system operations are consistent with organization-established recovery time objectives. Related control: CP-2.

Control Enhancements:

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

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

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

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

(5) **The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.**

LOW Not Selected	**MOD** CP-7 (1) (2) (3) (5)	**HIGH** CP-7 (1) (2) (3) (4) (5)

CP-8 TELECOMMUNICATIONS SERVICES

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

Supplemental Guidance: Related control: CP-2.

Control Enhancements:

(1) The organization:

(a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements; and

(b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

(2) The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.

Enhancement Supplemental Guidance: A full explanation of the Telecommunications Service Priority program is provided at http://tsp.ncs.gov.

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

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

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

CP-9 INFORMATION SYSTEM BACKUP

Control: The organization:

a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency*];

b. Conducts backups of system-level information (including system state information) contained in the information system [*Assignment: organization-defined frequency*]; and

c. Protects the confidentiality and integrity of backup information at the storage location.

Supplemental Guidance: The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the recovery time and recovery point objectives for the organization. Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by organizations to protect the integrity of information system backups. Protecting backup information from unauthorized disclosure is also an important consideration depending on the type of information residing on the backup media and the FIPS 199 impact level. An organizational assessment of risk guides the use of encryption for backup information. The protection of system backup information while in transit is beyond the scope of this control. Related controls: CP-6, MP-4, MP-5.

Control Enhancements:

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

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

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

(4) [Withdrawn: Incorporated into CP-9].

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

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Control: The organization provides the capability to recover and reconstitute the information system to a known secure state after a disruption, compromise, or failure.

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

Control Enhancements:

(1) [Withdrawn: Incorporated into CP-4].

(2) **The organization implements transaction recovery for information systems that are transaction-based (e.g., database management systems).**

Enhancement Supplemental Guidance: Transaction rollback and transaction journaling are examples of mechanisms supporting transaction recovery.

(3) **The organization provides compensating security controls (including procedures or mechanisms) for [*Assignment: organization-defined circumstances that inhibit recovery to a known, secure state*].**

(4) **The organization provides the capability to re-image information system components in accordance with [*Assignment: organization defined restoration time-periods*] from configuration controlled and integrity protected disk images representing a secure, operational state for the components.**

LOW CP-10	**MOD** CP-10	**HIGH** CP-10 (3) (4)

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

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

a. A formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

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

Control Enhancements: None.

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

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

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

Supplemental Guidance: Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Organizational users include federal employees and contractors. Access to organizational information systems is defined as either local or network. Local access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. Network access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained across a network connection. Remote access is a type of network access which involves communication through an external, non-organization-controlled network (e.g., the Internet). Organization-controlled networks include local area networks, wide area networks, and virtual private networks that are totally under the control of the organization. Identification and authentication requirements for information system access by other than organizational users are described in IA-8.

FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. The identification and authentication requirements in this control are satisfied by complying with FIPS 201 as required by Homeland Security Presidential Directive (HSPD) 12. The selection of authentication mechanisms specified in FIPS 201 is constrained by whether access to the organizational information system is local or network. FIPS 201 (Section 6.3.2) provides information on appropriate authentication mechanisms for local and network accesses to information systems. The use of FIPS 201 authentication mechanisms is consistent with organization-specific PIV implementation plans provided to OMB. In addition to identifying and authenticating users at the information system level (i.e., at system logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Related controls: AC-14, AC-17, IA-4, IA-5.

Control Enhancements:

(1) The information system employs multifactor authentication for remote access and for access to privileged accounts.

(2) The information system employs multifactor authentication for network access and for access to privileged accounts.

(3) The information system employs multifactor authentication for local and network access.

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

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: The information system uniquely identifies and authenticates [*Assignment: organization-defined list of devices*] before establishing a connection.

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

Control Enhancements:

(1) The information system authenticates devices before establishing remote network connections using bi-directional authentication between devices that is cryptographically based.

Enhancement Supplemental Guidance: Remote network connection is any connection with a device communicating through an external, non-organization-controlled network (e.g., the Internet).

(2) The information system authenticates devices before establishing network connections using bi-directional authentication between devices that is cryptographically based.

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

IA-4 IDENTIFIER MANAGEMENT

Control: The organization manages information system identifiers for users and devices by:

a. Receiving authorization from a designated organizational official to assign a user or device identifier;

b. Selecting an identifier that uniquely identifies an individual or device;

c. Assigning the user identifier to the intended party or the device identifier to the intended device; and

d. Archiving previous user or device identifiers.

Supplemental Guidance: Common device identifiers include media access control (MAC) or Internet protocol (IP) addresses, or device unique token identifiers. Management of user identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). It is commonly the case that a user identifier is the name of an information system account associated with an individual. In such instances, identifier management is largely addressed by the account management activities of AC-2. IA-4 also covers user identifiers not necessarily associated with an information system account (e.g., the identifier used in a physical security control database accessed by a badge reader system for access to the information system). FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. Related control: IA-2.

Control Enhancements: None.

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

IA-5 AUTHENTICATOR MANAGEMENT

Control: The organization manages information system authenticators for users and devices by:

a. Verifying, as part of the initial authenticator distribution for a user authenticator, the identity of the individual receiving the authenticator;

b. Establishing initial authenticator content for organization-defined authenticators;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators;

e. Changing default content of authenticators upon information system installation;

f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);

g. Changing/refreshing authenticators periodically, as appropriate for authenticator type;

h. Protecting authenticator content from unauthorized disclosure and modification; and

i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

Supplemental Guidance: Device authenticators include, for example, certificates and passwords. User authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many information system components are shipped with factory default user authentication credentials to allow for initial installation and configuration. However, factory default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore are changed upon installation. The requirement to protect user authenticators may be implemented via control PL-4 or PS-6. The information system supports user authenticator management requirements by enforcing organization-defined password minimum and maximum lifetime restrictions and password reuse restrictions for organization-defined number of generations. Measures to safeguard user authenticators includes, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems (and associated authenticator management) may also be required to protect nonpublic or privacy-related information. FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. Related controls: IA-2, PL-4, PL-6.

Control Enhancements:

(1) The information system, for PKI-based authentication:

(a) Validates certificates by constructing a certification path with status information to an accepted trust anchor;

(b) Enforces authorized access to the corresponding private key; and

(c) Maps the authenticated identity to the user account.

Enhancement Supplemental Guidance: Status information for certification paths includes, for example, certificate revocation lists or online certificate status protocol responses.

(2) The organization requires that the registration process to receive a user authenticator be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).

(3) The organization employs automated tools to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators.

(4) The organization requires unique authenticators be provided by vendors and/or manufacturers of information system components.

LOW IA-5	**MOD** IA-5 (1)	**HIGH** IA-5 (1)

IA-6 AUTHENTICATOR FEEDBACK

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

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

Control Enhancements: None.

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

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

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

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

Control Enhancements: None.

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

IA-8 IDENTIFICATION AND AUTHENTICATION (NON ORGANIZATIONAL USERS)

Control: The information system uniquely identifies and authenticates non organizational users (or processes acting on behalf of non organizational users) for remote access.

Supplemental Guidance: In accordance with OMB policy and E-Authentication E-Government initiative, authentication of non organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information. Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance with security control AC-14. Non organizational users include all information system users other than federal employees and contractors explicitly covered by IA-2. Remote access is a type of network access which involves communication through an external, non-organization-controlled network (e.g., the Internet).

The E-authentication risk assessment conducted in accordance with OMB Memorandum 04-04 is used in determining the authentication needs of non organizational users based on risks, potential impacts, and required assurance levels. Scalability, practicality, and security issues are simultaneously considered in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. NIST Special Publication 800-63 provides technical guidelines to organizations for the implementation of E-authentication. Identification and authentication requirements for information system access by organizational users are described in IA-2. Related control: AC-14.

Control Enhancements: None.

LOW IA-8	**MOD** IA-8	**HIGH** IA-8

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

a. A formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

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

Control Enhancements: None.

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

IR-2 INCIDENT RESPONSE TRAINING

Control: The organization:

a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and

b. Provides refresher training [*Assignment: organization-defined frequency, at least annually*].

Supplemental Guidance: None.

Control Enhancements:

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

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

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

IR-3 INCIDENT RESPONSE TESTING AND EXERCISES

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

Supplemental Guidance: NIST Special Publication 800-84 provides guidance on testing, training, and exercise programs for information technology plans and capabilities. NIST Special Publication 800-115 provides guidance on security testing and assessment.

Control Enhancements:

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

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

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

IR-4 INCIDENT HANDLING

Control: The organization:

a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and

b. Coordinates incident handling activities with contingency planning activities; and

c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures and implements the procedures accordingly.

Supplemental Guidance: NIST Special Publication 800-61 provides guidance on incident handling. Related controls: AU-6, CA-2, CP-2, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

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

Enhancement Supplemental Guidance: An online, incident management system is an example of an automated mechanism.

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

IR-5 INCIDENT MONITORING

Control: The organization tracks and documents information system security incidents.

Supplemental Guidance: Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Control Enhancements:

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

Enhancement Supplemental Guidance: The Einstein network monitoring device from the Department of Homeland Security is an example of an automated mechanism.

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

IR-6 INCIDENT REPORTING

Control: The organization reports security incident information to designated authorities.

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

Control Enhancements:

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

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

IR-7 INCIDENT RESPONSE ASSISTANCE

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

Supplemental Guidance: Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required. Related controls: IR-4, IR-6.

Control Enhancements:

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

Enhancement Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

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

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

a. A formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.

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

Control Enhancements: None.

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

MA-2 CONTROLLED MAINTENANCE

Control: The organization:

a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Explicitly approves the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

c. Sanitizes the equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and

d. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

Supplemental Guidance: The control is intended to address the information security aspects of the organization's information system maintenance program. All maintenance activities to include routine, scheduled maintenance and repairs are controlled; whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. Related controls: MP-6, SI-2.

Control Enhancements:

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

(2) **The organization employs automated mechanisms to schedule and document maintenance and repairs as required, producing up-to date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed.**

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

MA-3 MAINTENANCE TOOLS

Control: The organization approves and monitors the use of information system maintenance tools.

Supplemental Guidance: The intent of this control is to address the security-related issues arising from the hardware and software brought into the information system specifically for diagnostic and repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control. Related control: MP-6.

Control Enhancements:

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

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

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

(3) The organization prevents the unauthorized removal of maintenance equipment by one of the following: (i) verifying that there is no organizational information contained on the equipment; (ii) sanitizing or destroying the equipment; (iii) retaining the equipment within the facility; or (iv) obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.

Enhancement Supplemental Guidance: NIST Special Publication 800-88 provides guidance on media sanitization. The National Security Agency provides a listing of approved media sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

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

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

MA-4 REMOTE MAINTENANCE

Control: The organization:

a. Authorizes and monitors remotely executed maintenance and diagnostic activities, if employed;

b. Allows the use of remote maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;

c. Maintains records for remote maintenance and diagnostic activities; and

d. Terminates all sessions and remote connections when remote maintenance is completed; and

e. Changes passwords following each remote maintenance session, if password-based authentication is used to accomplish remote maintenance.

Supplemental Guidance: Remote maintenance and diagnostic activities are conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). Other techniques and/or measures to consider for improving the security of remote maintenance include: (i) encryption and decryption of communications; (ii) strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST Special Publication 800-63; and (iii) remote disconnect verification. Related controls: IA-2, MP-6.

Control Enhancements:

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

(2) The organization documents the installation and use of remote maintenance and diagnostic links.

(3) The organization:

(a) Requires that remote maintenance or diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or

(b) Removes the component to be serviced from the information system and prior to remote maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities and after the service is performed, sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.

Enhancement Supplemental Guidance: NIST Special Publication 800-88 provides guidance on media sanitization. The National Security Agency provides a listing of approved media sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

(4) The organization requires that remote maintenance sessions are protected through the use of a strong authenticator tightly bound to the user.

Enhancement Supplemental Guidance: Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, pass-phrase or biometric.

(5) The organization requires that: (i) maintenance personnel notify the system administrator when remote maintenance is planned (i.e., date/time); and (ii) a designated organizational official with specific information security/information system knowledge approves the remote maintenance.

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

MA-5 MAINTENANCE PERSONNEL

Control: The organization:

a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel;

b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.

Supplemental Guidance: None.

Control Enhancements: None.

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

MA-6 TIMELY MAINTENANCE

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

Supplemental Guidance: The organization specifies those information system components that, when not operational, result in increased risk to organizations, individuals, or the Nation because the security functionality intended by that component is not being provided. Security-critical components include, for example, firewalls, guards, gateways, intrusion detection systems, audit repositories, authentication servers, and intrusion prevention systems.

Control Enhancements: None.

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

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

a. A formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

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

Control Enhancements: None.

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

MP-2 MEDIA ACCESS

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

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

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection. Related control: MP-4.

Control Enhancements:

(1) The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

Enhancement Supplemental Guidance: This control enhancement is primarily applicable to designated media storage areas within an organization where a significant volume of media is stored and is not intended to apply to every location where some media is stored (e.g., in individual offices).

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

MP-3 MEDIA MARKING

Control: The organization:

a. Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and

b. Exempts [*Assignment: organization-defined list of media types or hardware components*] from marking as long as the exempted items remain within [*Assignment: organization-defined protected environment*].

Supplemental Guidance: The term marking is distinguished from the term labeling. Marking is used in security controls when referring to information that is human-readable. The term labeling is used in the context of marking internal data structures within the information system (e.g., AC-16, Automated Labeling) for access control purposes for information in process, in storage, or in transit. Removable information system media includes both digital media (e.g., magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks, diskettes) and non-digital media (e.g., paper, microfilm). An organizational assessment of risk guides the selection of media requiring marking. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, marking is not required for media containing information determined by the organization to be in the public domain or to be publicly releasable.

Control Enhancements:

(1) The information system marks output on external media including video display devices, to identify any of the [*Assignment: organization-identified set of special dissemination, handling, or distribution instructions*] that apply to system output using [*Assignment: organization-identified human readable, standard naming conventions*].

Enhancement Supplemental Guidance: Information system markings refer to the markings employed on external media (e.g., video displays, hardcopy documents output from the information system). External markings are distinguished from internal markings (i.e., the labels used on internal data structures within the information system described in AC-16). Video display devices include, for example, computer terminals, monitors, screens on notebook computers and personal digital assistants.

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

MP-4 MEDIA STORAGE

Control: The organization physically protects and securely stores information system media within [*Assignment: organization-defined controlled areas*].

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control applies to mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Organizations document in policy and procedures, the media requiring physical protection and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection. The organization protects information system media identified by the organization until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

As part of a defense-in-depth protection strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. FIPS 199 security categorization guides the selection of appropriate candidates for secondary storage encryption. The organization implements effective cryptographic key management in support of secondary storage encryption and provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users. NIST Special Publications 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Related controls: AC-19, CP-6, CP-9, MP-2.

Control Enhancements: None.

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

MP-5 MEDIA TRANSPORT

Control: The organization:

a. Protects [*Assignment: organization-defined types of digital and non-digital media*] during transport outside of controlled areas using [*Assignment: organization-defined security measures*];

b. Maintains accountability for information system media during transport outside of controlled areas; and

c. Restricts the activities associated with transport of such media to authorized personnel.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

Physical and technical security measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FIPS 199 security categorization of the information residing on the media, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Locked containers and cryptography are examples of security measures available to protect digital and non-digital media during transport. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used. An organizational assessment of risk guides the selection of media and associated information contained on that media requiring protection during transport. Organizations document in policy and procedures, the media requiring protection during transport and the specific measures taken to protect such transported media. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. An organizational assessment of risk also guides the selection and use of storage containers for transporting non-digital media. Authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Related controls: AC-19, CP-9.

Control Enhancements:

(1) [Withdrawn: Incorporated into MP-5].

(2) The organization documents activities associated with the transport of information system media using [*Assignment: organization-defined system of records*].

Enhancement Supplemental Guidance: Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk.

(3) The organization employs an identified custodian throughout the transport of information system media.

Enhancement Supplemental Guidance: Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.

LOW Not Selected	**MOD** MP-5 (2)	**HIGH** MP-5 (2) (3)

MP-6 MEDIA SANITIZATION

Control: The organization sanitizes information system media, both digital and non-digital, prior to disposal or release for reuse.

Supplemental Guidance: This control applies to all media subject to disposal or reuse, whether or not considered removable. Sanitization is the process used to remove information from information system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or disposed of. The organization employs sanitization mechanisms with strength and integrity commensurate with the security category of the information. FIPS 199 and NIST Special Publication 800-60 provide standards and guidance on security categories of federal information and information systems. The organization uses its discretion on the use of sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposed. NIST Special Publication 800-88 provides guidance on media sanitization. The National Security Agency also provides media sanitization guidance and maintains a listing of approved sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

Control Enhancements:

(1) The organization tracks, documents, and verifies media sanitization actions.

(2) The organization periodically tests sanitization equipment and procedures to verify correct performance.

LOW MP-6	**MOD** MP-6	**HIGH** MP-6 (1) (2)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

a. A formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

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

Control Enhancements: None.

LOW PE-1	**MOD** PE-1	**HIGH** PE-1

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control: The organization:

a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);

b. Issues authorization credentials;

c. Reviews and approves the access list and authorization credentials [*Assignment: organization-defined frequency, at least annually*], removing from the access list, personnel no longer requiring access.

Supplemental Guidance: Authorization credentials include, for example, badges, identification cards, and smart cards. Related control: PE-3, PE-4.

Control Enhancements:

(1) The organization authorizes physical access to the facility where the information system resides based upon position or role.

(2) The organization requires two forms of identification to gain access to the facility where the information system resides.

Enhancement Supplemental Guidance: Examples of forms of identification are identification badge, key card, cipher PIN, and biometrics.

LOW PE-2	**MOD** PE-2	**HIGH** PE-2

PE-3 PHYSICAL ACCESS CONTROL

Control: The organization:

a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);

b. Verifies individual access authorizations before granting access to the facility;

c. Controls entry to facilities containing information systems using physical access devices and/or guards;

d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;

e. Secures keys, combinations, and other physical access devices;

f. Inventories physical access devices [*Assignment: organization-defined frequency*]; and

g. Changes combinations and keys [*Assignment: organization-defined frequency*] and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Supplemental Guidance: Physical access devices include, for example, keys, locks, combinations, card readers. 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 safeguarded. Where federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST Special Publication 800-73. If the token-based access control function employs cryptographic verification, the access control system conforms to the requirements of NIST Special Publication 800-78. If the token-based access control function employs biometric verification, the access control system conforms to the requirements of NIST Special Publication 800-76. Related control: PE-2.

Control Enhancements:

(1) The organization enforces physical access authorizations to the information system independent of the physical access controls for the facility.

Enhancement Supplemental Guidance: This control enhancement, in general, applies to server rooms, communications centers, or any other areas within a facility containing large concentrations of information system components or components with a higher impact level than that of the majority of the facility. The intent is to provide an additional layer of physical security for those areas where the organization may be more vulnerable due to the concentration of information system components or the impact level of the components. The control enhancement is not intended to apply to workstations or peripheral devices that are typically dispersed throughout the facility and used routinely by organizational personnel.

(2) The organization performs security checks at physical boundaries for unauthorized exfiltration of information or information system components.

Enhancement Supplemental Guidance: The extent and frequency or randomness of these checks is as deemed necessary by the organization to adequately mitigate the risk associated with exfiltration.

(3) The organization ensures that every physical access point to the facility where the information system resides is guarded or alarmed and monitored 24 hours per day, 7 days per week.

(4) The organization employs lockable physical casings to protect internal components of the information system from unauthorized physical access.

(5) The information system employs mechanisms that: (i) detect physical tampering; or (ii) prevent physical tampering or alteration of hardware components within the system.

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

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities.

Supplemental Guidance: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Related control: PE-2.

Control Enhancements: None.

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

PE-5 ACCESS CONTROL FOR DISPLAY MEDIUM

Control: The organization controls physical access to information system display devices to prevent unauthorized individuals from observing the display output.

Supplemental Guidance: A monitor is an example of an information system device that displays information.

Control Enhancements: None.

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

PE-6 MONITORING PHYSICAL ACCESS

Control: The organization:

a. Monitors physical access to the information system to detect and respond to physical security incidents;

b. Reviews physical access logs [*Assignment: organization-defined frequency*]; and

c. Coordinates results of reviews and investigations with the organization’s incident response capability.

Supplemental Guidance: Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization’s incident response capability.

Control Enhancements:

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

(2) The organization employs automated mechanisms to recognize potential intrusions and initiate designated response actions.

LOW PE-6	**MOD** PE-6 (1)	**HIGH** PE-6 (1) (2)

PE-7 VISITOR CONTROL

Control: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.

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

Control Enhancements:

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

(2) The organization requires two forms of identification for access to the facility.

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

PE-8 ACCESS RECORDS

Control: The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the visitor access records [*Assignment: organization-defined frequency*].

Supplemental Guidance: None.

Control Enhancements:

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

(2) The organization maintains a record of all physical access, both visitor and authorized individuals.

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

PE-9 POWER EQUIPMENT AND POWER CABLING

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

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs redundant and parallel power cabling paths.

LOW Not Selected	**MOD** PE-9	**HIGH** PE-9

PE-10 EMERGENCY SHUTOFF

Control: The organization, for specific locations within a facility containing concentrations of information system resources, protects emergency power shutoff capability from unauthorized activation.

Supplemental Guidance: Facilities containing concentrations of information system resources may include, for example, data centers, server rooms, and mainframe rooms.

Control Enhancements:

(1) [Withdrawn: Incorporated into PE-10].

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

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: This control may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations should avoid duplicating actions already covered.

Control Enhancements:

(1) **The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.**

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

LOW Not Selected	**MOD** PE-11	**HIGH** PE-11 (1)

PE-12 EMERGENCY LIGHTING

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

Supplemental Guidance: This control may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations should avoid duplicating actions already covered.

Control Enhancements: None.

LOW PE-12	**MOD** PE-12	**HIGH** PE-12

PE-13 FIRE PROTECTION

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

Supplemental Guidance: Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors. This control may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations should avoid duplicating actions already covered.

Control Enhancements:

(1) The organization employs fire detection devices/systems that activate automatically and notify the organization and emergency responders in the event of a fire.

(2) The organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders.

(3) The organization employs an automatic fire suppression capability in facilities that are not staffed on a continuous basis.

LOW PE-13	**MOD** PE-13 (1) (2) (3)	**HIGH** PE-13 (1) (2) (3)

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control: The organization:

a. Maintains temperature and humidity levels within the facility where the information system resides at [*Assignment: organization-defined acceptable levels*]; and

b. Monitors temperature and humidity levels [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations should avoid duplicating actions already covered.

Control Enhancements: None.

LOW PE-14	**MOD** PE-14	**HIGH** PE-14

PE-15 WATER DAMAGE PROTECTION

Control: The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

Supplemental Guidance: This control may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations should avoid duplicating actions already covered.

Control Enhancements:

(1) The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a water leak.

LOW PE-15	**MOD** PE-15	**HIGH** PE-15 (1)

PE-16 DELIVERY AND REMOVAL

Control: The organization authorizes and monitors [*Assignment: organization-defined types of information system components*] entering and exiting the facility and maintains records of those items.

Supplemental Guidance: Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

Control Enhancements: None.

LOW PE-16	**MOD** PE-16	**HIGH** PE-16

PE-17 ALTERNATE WORK SITE

Control: The organization:

a. Employs [*Assignment: organization-defined management, operational, and technical information system security controls*] at alternate work sites; and

b. Monitors the effectiveness of security controls at alternate work sites.

Supplemental Guidance: Alternate work sites may, for example, include government facilities or private residences of employees. The organization may define different sets of security controls for specific alternate work sites or types of sites. NIST Special Publication 800-46 provides guidance on security in telecommuting and broadband communications.

Control Enhancements: None.

LOW Not Selected	**MOD** PE-17	**HIGH** PE-17

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

Control: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards. This control may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations should avoid duplicating actions already covered

Control Enhancements:

(1) The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

LOW Not Selected	**MOD** PE-18	**HIGH** PE-18 (1)

PE-19 INFORMATION LEAKAGE

Control: The organization protects the information system from information leakage due to electromagnetic signals emanations.

Supplemental Guidance: The FIPS 199 security categorization (for confidentiality) of the information system and organizational security policy guides the application of safeguards and countermeasures employed to protect the information system against information leakage due to electromagnetic signals emanations.

Control Enhancements: None.

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

FAMILY: PLANNING **CLASS:** MANAGEMENT

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

a. A formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

Supplemental Guidance: The security planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-18 provides guidance on security planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW PL-1	**MOD** PL-1	**HIGH** PL-1

PL-2 SYSTEM SECURITY PLAN

Control: The organization:

a. Develops a security plan for the information system that:

- Aligns with the organization's enterprise architecture;
- Explicitly defines the authorization boundary for the system;
- Describes relationships with or connections to other information systems;
- Provides an overview of the security requirements for the system;
- Describes the security controls in place or planned for meeting those requirements; and
- Is reviewed and approved by the authorizing official or authorizing official designated representative prior to plan implementation.

b. Reviews the security plan for the information system [*Assignment: organization-defined frequency, at least annually*]; and

c. Revises the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

Supplemental Guidance: The security plan contains sufficient information (including specification of parameters for assignment and selection statements in security controls either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a subsequent determination of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Security plans are reviewed and approved by authorizing officials or authorizing official designated representatives prior to implementation as part of an organizational risk management strategy. NIST Special Publication 800-18 provides guidance on security planning.

Control Enhancements: None.

LOW PL-2	**MOD** PL-2	**HIGH** PL-2

PL-3 SYSTEM SECURITY PLAN UPDATE

[Withdrawn: Incorporated into PL-2].

PL-4 RULES OF BEHAVIOR

Control: The organization:

a. Establishes and makes readily available to all information system users, a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage; and

b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

Supplemental Guidance: Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy. NIST Special Publication 800-18 provides guidance on preparing rules of behavior. Related control: PS-6.

Control Enhancements:

(1) The organization includes in the rules of behavior, explicit restrictions on the use of social networking sites, posting information on commercial web sites, and sharing information system account information.

LOW PL-4	**MOD** PL-4	**HIGH** PL-4

PL-5 PRIVACY IMPACT ASSESSMENT

Control: The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.

Supplemental Guidance: OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002. NIST Special Publication 800-122 provides guidance on protecting the confidentiality of personally identifiable information.

Control Enhancements: None.

LOW PL-5	**MOD** PL-5	**HIGH** PL-5

PL-6 SECURITY-RELATED ACTIVITY PLANNING

Control: The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

Supplemental Guidance: Security-related activities include, for example, security assessments, audits, system hardware and software maintenance, and contingency plan testing/exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., planned or nonurgent unplanned) situations.

Control Enhancements: None.

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

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

a. A formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

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

Control Enhancements: None.

LOW PS-1	**MOD** PS-1	**HIGH** PS-1

PS-2 POSITION CATEGORIZATION

Control: The organization:

a. Assigns a risk designation to all positions;

b. Establishes screening criteria for individuals filling those positions; and

c. Reviews and revises position risk designations [*Assignment: organization-defined frequency*].

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

Control Enhancements: None.

LOW PS-2	**MOD** PS-2	**HIGH** PS-2

PS-3 PERSONNEL SCREENING

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

Supplemental Guidance: Screening is consistent with: (i) 5 CFR 731.106; (ii) Office of Personnel Management policy, regulations, and guidance; (iii) organizational policy, regulations, and guidance; (iv) FIPS 201 and Special Publications 800-73, 800-76, and 800-78; and (v) the criteria established for the risk designation of the assigned position.

Control Enhancements:

(1) The organization re-screens individuals with access to organizational information systems [*Assignment: organization-defined list of conditions requiring rescreening and the frequency of such rescreening*].

Enhancement Supplemental Guidance: The organization may define different rescreening conditions and frequencies for personnel accessing organizational information systems in accordance with the FIPS 199 security categorization of the system.

LOW PS-3	**MOD** PS-3	**HIGH** PS-3

PS-4 PERSONNEL TERMINATION

Control: The organization upon termination of individual employment:

a. Terminates information system access;

b. Conducts exit interviews;

c. Retrieves all security-related organizational information system-related property; and

d. Retains access to organizational information and information systems formerly controlled by terminated individual.

Supplemental Guidance: Information system-related property includes, for example, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that individuals understand any security constraints imposed by being former employees and that proper accountability is achieved for all information system-related property. Timely execution of this control is particularly essential for employees or contractors terminated for cause.

Control Enhancements: None.

LOW PS-4	**MOD** PS-4	**HIGH** PS-4

PS-5 PERSONNEL TRANSFER

Control: The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates [*Assignment: organization-defined transfer or reassignment actions*].

Supplemental Guidance: Actions that may be required when personnel are transferred or reassigned to other positions within the organization include, for example: (i) returning old and issuing new keys, identification cards, building passes; (ii) closing previous information system accounts and establishing new accounts; (iii) changing information system access authorizations; and (iv) providing for access to official records to which the employee had access at the previous work location and in the previous information system accounts.

Control Enhancements: None.

LOW PS-5	**MOD** PS-5	**HIGH** PS-5

PS-6 ACCESS AGREEMENTS

Control: The organization:

a. Completes signed access agreements for individuals requiring access to organizational information and information systems prior to authorizing access; and

b. Reviews/updates the access agreements [*Assignment: organization-defined frequency*].

Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the information system to which access is authorized. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy. Related control: PL-4.

Control Enhancements: None.

LOW PS-6	**MOD** PS-6	**HIGH** PS-6

PS-7 THIRD-PARTY PERSONNEL SECURITY

Control: The organization establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance.

Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents. NIST Special Publication 800-35 provides guidance on information technology security services.

Control Enhancements: None.

LOW PS-7	**MOD** PS-7	**HIGH** PS-7

PS-8 PERSONNEL SANCTIONS

Control: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Supplemental Guidance: The sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The sanctions process can be included as part of the general personnel policies and procedures for the organization.

Control Enhancements: None.

LOW PS-8	**MOD** PS-8	**HIGH** PS-8

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

Supplemental Guidance: The risk assessment policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-30 provides guidance on the assessment of risk. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW RA-1	**MOD** RA-1	**HIGH** RA-1

RA-2 SECURITY CATEGORIZATION

Control: The organization categorizes information and information systems in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance and documents the results (including supporting rationale) in the system security plan.

Supplemental Guidance: The applicable federal standard for security categorization of nonnational security information and information systems is FIPS 199. The organization conducts FIPS 199 security categorizations as an organization-wide activity with the involvement of the chief information officer, senior information security officer, information system owners, and information owners/stewards. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and restricting or prohibiting network access in accordance with an organizational assessment of risk. Security categorization decisions are reviewed and approved by authorizing officials or authorizing official designated representatives prior to implementation as part of an organizational risk management strategy. NIST Special Publication 800-60 provides guidance on determining the security categories of the information types resident on the information system. Related controls: MP-4, SC-7.

Control Enhancements: None.

LOW RA-2	**MOD** RA-2	**HIGH** RA-2

RA-3 RISK ASSESSMENT

Control: The organization:

a. Conducts assessments of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization; and

b. Updates risk assessments [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation, or other conditions that may impact the security state of the system.

Supplemental Guidance: Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems. NIST Special Publication 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments.

Control Enhancements: None.

LOW RA-3	**MOD** RA-3	**HIGH** RA-3

RA-4 RISK ASSESSMENT UPDATE

[Withdrawn: Incorporated into RA-3].

RA-5 VULNERABILITY SCANNING

Control: The organization:

a. Scans for vulnerabilities in the information system [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system are identified and reported;

b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:

- Enumerating platforms, software flaws, and improper configurations;
- Formatting and making transparent, checklists and test procedures; and
- Measuring vulnerability impact;

c. Analyzes vulnerability scan reports and remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] and organizational assessment of risk; and

d. Shares information obtained from the vulnerability scanning process with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems.

Supplemental Guidance: Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools to scan for web-based vulnerabilities, source code reviews, static analysis of source code). Vulnerability scanning includes scanning for ports, protocols, and services that should not be accessible to users and for improperly configured or incorrectly operating information flow mechanisms. NIST Special Publication 800-42 provides guidance on network security testing. NIST Special Publication 800-40 provides guidance on patch and vulnerability management. Related control: SI-2.

Control Enhancements:

(1) **The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.**

(2) **The organization updates the list of information system vulnerabilities scanned [*Assignment: organization-defined frequency*] or when new vulnerabilities are identified and reported.**

(3) **The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).**

(4) **The organization attempts to discern what information about the information system is discoverable by adversaries.**

(5) **The organization performs security testing to determine the level of difficulty in circumventing the security controls of the information system.**

Enhancement Supplemental Guidance: Testing methods include, for example, penetration testing, malicious user testing, and independent verification and validation (IV&V). Testing is conducted in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards. Testing methods are approved by Authorizing Officials in coordination with the organization's Risk Executive Function.

(6) **The organization includes privileged access authorization to [*Assignment: organization-defined information system components*] for selected vulnerability scanning activities to facilitate more thorough scanning.**

(7) **The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.**

(8) **The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials.**

LOW RA-5	**MOD** RA-5 (1)	**HIGH** RA-5 (1) (2) (3) (4) (5) (8)

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

a. A formal, documented, system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. 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 laws, Executive Orders, 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.

LOW SA-1	**MOD** SA-1	**HIGH** SA-1

SA-2 ALLOCATION OF RESOURCES

Control: The organization:

a. Includes a determination of information security requirements for the information system in mission/business case planning; and

b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process.

Supplemental Guidance: NIST Special Publication 800-65 provides guidance on integrating security into the capital planning and investment control process. Related controls: PM-3, PM-11.

Control Enhancements: None.

LOW SA-2	**MOD** SA-2	**HIGH** SA-2

SA-3 LIFE CYCLE SUPPORT

Control: The organization manages the information system using a system development life cycle methodology that includes information security considerations.

Supplemental Guidance: NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle. Related control: PM-7.

Control Enhancements: None.

LOW SA-3	**MOD** SA-3	**HIGH** SA-3

SA-4 ACQUISITIONS

Control: The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards:

- Security functional requirements/specifications;
- Security-related documentation requirements; and
- Developmental and evaluation-related assurance requirements.

Supplemental Guidance: The acquisition documents for information systems and services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. NIST Special Publication 800-36 provides guidance on the selection of information security products. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle. NIST Special Publication 800-23 provides guidance on the acquisition and use of tested/evaluated information technology products. NIST Special Publication 800-70 provides guidance on configuration settings for information technology products.

Control Enhancements:

(1) The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls employed within the information system.

(2) The organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls employed within the information system (including functional interfaces among control components).

(3) The organization limits the acquisition of commercial information technology products with security capabilities to products which have been evaluated and validated through a government-approved process.

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

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control: The organization:

a. Obtains, protects as required, and makes available to authorized personnel, administrator and user guidance for the information system that includes information on: (i) configuring, installing, and operating the information system; and (ii) using the system's security features; or

b. Documents attempts to obtain information system documentation when such documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/contractor) and provides compensating security controls, if needed.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization obtains, if available from the vendor/contractor, information describing the functional properties of the security controls employed within the information system.

(2) The organization obtains, if available from the vendor/contractor, information describing the design and implementation details of the security controls employed within the information system (including functional interfaces among control components).

(3) The organization obtains, if available from the vendor/contractor, information that describes the security-relevant external interfaces to the information system.

LOW SA-5	**MOD** SA-5 (1) (3)	**HIGH** SA-5 (1) (2) (3)

SA-6 SOFTWARE USAGE RESTRICTIONS

Control: The organization:

a. Uses software and associated documentation in accordance with contract agreements and copyright laws;

b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and

c. 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.

Supplemental Guidance: None.

Control Enhancements: None.

LOW SA-6	**MOD** SA-6	**HIGH** SA-6

SA-7 USER INSTALLED SOFTWARE

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

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect). Related control: CM-2.

Control Enhancements: None.

LOW SA-7	**MOD** SA-7	**HIGH** SA-7

SA-8 SECURITY ENGINEERING PRINCIPLES

Control: The organization applies information system security engineering principles in the specification, design, development, and implementation of the information system.

Supplemental Guidance: NIST Special Publication 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.

Control Enhancements: None.

LOW Not Selected	**MOD** SA-8	**HIGH** SA-8

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

Control: The organization:

a. Requires that providers of external information system services employ security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements;

b. Defines government oversight and user roles and responsibilities with regard to external information system services; and

c. Monitors security control compliance by external service providers.

Supplemental Guidance: An external information system service is a service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. Ultimately, the responsibility for adequately mitigating risks arising from the use of external information system services remains with the authorizing official. Authorizing officials must require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information system security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. The extent and nature of this chain of trust varies based upon the relationship between the organization and the external provider. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk to its operations and assets, or to individuals. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance. NIST Special Publication 800-35 provides guidance on information technology security services.

Control Enhancements: None.

LOW SA-9	**MOD** SA-9	**HIGH** SA-9

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Control: The organization requires that information system developers/integrators implement and document a configuration management process that: (i) manages and controls changes to the system during design, development, implementation, and operation; (ii) tracks security flaws; and (iii) includes organizational approval of changes.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization requires that information system developers/integrators provide an integrity check of software to facilitate organizational verification of software integrity after delivery.

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

SA-11 DEVELOPER SECURITY TESTING

Control: The organization requires that information system developers/integrators create a security test and evaluation plan, implement the plan, and document the results.

Supplemental Guidance: Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security-relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security authorization process for the delivered information system. Related controls: CA-2.

Control Enhancements:

(1) The organization requires that information system developers/integrators employ code analysis tools to examine software for common flaws and document the results of the analysis.

(2) The organization requires that information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.

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

SA-12 SUPPLY CHAIN PROTECTION

Control: The organization protects against supply chain threats by employing: [*Assignment: organization-defined list of measures to protect against supply chain threats*].

Supplemental Guidance: A supply chain is a system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers. Products and services in the domestic and international supply chain include, for example, hardware, software, and firmware components for information systems, data management services, telecommunications service providers, and Internet service providers. Domestic and international supply chains are becoming increasingly important to the national and economic security interests of the United States because of the growing dependence on products and services produced or maintained in worldwide markets. Uncertainty in the supply chain and the growing sophistication and diversity of international cyber threats increase the potential for a range of adverse effects on organizational operations and assets, individuals, other organizations, and the Nation. Global commercial supply chains provide adversaries with opportunities to manipulate information technology products that are routinely used by public and private sector organizations (e.g., federal agencies, contractors) in the information systems that support U.S. critical infrastructure applications. Malicious activity at any point in the supply chain poses downstream risks to the mission/business processes that are supported by those information systems. To mitigate risk from the supply chain, a comprehensive information security strategy should be considered that employs a strategic, organization-wide *defense-in-breadth* approach. A defense-in-breadth approach helps to protect information systems (including the information technology products that compose those systems) throughout the SDLC (i.e., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). This is accomplished by the identification, management, and elimination of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to mitigate risk.

Control Enhancements:

(1) The organization employs anonymous contracting and acquisition vehicles.

Enhancement Supplemental Guidance: The organization can reduce the chance of targeted supply chain attacks during design, manufacture, or delivery by protecting the true identity of the ultimate customer through the use of anonymous contracting and acquisition vehicles.

(2) The organization purchases all anticipated information system components and spares in the initial acquisition.

Enhancement Supplemental Guidance: Stockpiling information system components and spares avoids the need to use less trustworthy secondary or resale markets in future years.

(3) The organization employs trusted cutouts for purchasing contract services, acquisitions, or logistical activities during the information system lifecycle.

Enhancement Supplemental Guidance: A trusted cutout is an individual or organization which can securely support logistical or acquisition activities without revealing the true identity of the requesting organization or the destination of the information system component or product. The organization can protect against an adversary targeting the manufacture or delivery of a information system component or product by encoding customer identity until the component or product arrives at the final stage of transport, at which point it can be handled by a trusted cutout.

(4) The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.

Enhancement Supplemental Guidance: The organization reviews supplier claims with regard to the use of appropriate security processes in the development and manufacture of information system components or products.

(5) The organization uses trusted shipping and warehousing for information systems, information system components, and information technology products.

Enhancement Supplemental Guidance: Trusted shipping and warehousing reduces opportunities for subversive activities or interception during transit.

(6) The organization uses a diverse set of suppliers for information systems, information system components, information technology products, and information system services.

Enhancement Supplemental Guidance: Diversification of suppliers is intended to limit the potential harm from a given supplier in a supply chain, increasing the work factor for an adversary.

(7) The organization uses standard configurations for information systems, information system components, and information technology products.

Enhancement Supplemental Guidance: By avoiding the purchase of custom configurations for information systems, information system components, and information technology products, the organization limits the possibility of acquiring systems and products that have been corrupted via the supply chain actions targeted at the organization.

(8) The organization minimizes the time between purchase decisions and delivery of information systems, information system components, and information technology products.

Enhancement Supplemental Guidance: By minimizing the time between purchase decisions and required delivery of information systems, information system components, and information technology products, the organization limits the opportunity for an adversary to corrupt the purchased system, component, or product.

(9) The organization employs independent analysis and penetration testing against delivered information systems, information system components, and information technology products.

LOW Not Selected	**MOD** Not Selected	**HIGH** SA-12

SA-13 TRUSTWORTHINESS

Control: The organization requires that the information system meets [*Assignment: organization-defined level of trustworthiness*].

Supplemental Guidance: The level of trustworthiness for organizational information systems is defined in terms of degree of correctness for intended functionality and of degree of resilience to attack by explicitly identified levels of adversary capability. In addition, but not as a replacement for this expression of degree of correctness and resilience, the level of trustworthiness may also be described in terms of levels of developmental assurance, that is, actions taken in the specification, design, development, implementation, and operation/maintenance of the information system that impact the degree of correctness and resilience achieved. Trustworthiness may be defined as different levels on the basis of component-by-component, subsystem-by-subsystem, function-by-function, or a combination of the above. It is noted, however, that typically functions, subsystems, and components are highly interrelated, making separation by trustworthiness perhaps problematic and at a minimum, something that likely requires careful attention in order to achieve practically useful results. Minimum assurance requirements are described in Appendix E. Related controls: SA-8, SC-3.

Control Enhancements:

(1) The organization requires that software developers employ software quality and validation methods to minimize flawed or malformed software.

LOW Not Selected	**MOD** Not Selected	**HIGH** SA-13

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates to [*Assignment: organization-defined list of appropriate organizational elements*], and periodically reviews/updates:

a. A formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

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

Control Enhancements: None.

LOW SC-1	**MOD** SC-1	**HIGH** SC-1

SC-2 APPLICATION PARTITIONING

Control: The information system separates user functionality (including user interface services) from information system management functionality.

Supplemental Guidance: The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-2	**HIGH** SC-2

SC-3 SECURITY FUNCTION ISOLATION

Control: The information system isolates security functions from nonsecurity functions.

Supplemental Guidance: The information system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions and domains) that controls access to and protects the 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. Related control: SA-13.

Control Enhancements:

(1) The information system employs underlying hardware separation mechanisms to facilitate security function isolation.

(2) The information system isolates security functions enforcing access and information flow control from both nonsecurity functions and from other security functions.

(3) The organization implements an information system isolation boundary to minimize the number of nonsecurity functions included within the boundary containing security functions.

Enhancement Supplemental Guidance: Nonsecurity functions contained within the isolation boundary are considered security relevant.

(4) The organization implements security functions as largely independent modules that avoid unnecessary interactions between modules.

(5) The organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

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

SC-4 INFORMATION IN SHARED RESOURCES

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

Supplemental Guidance: The purpose of this control is to prevent 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 of information in shared resources is also referred to as object reuse. This control does not address: (i) information remanence which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the information system for which there is only a single user/role.

Control Enhancements: None.

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

SC-5 DENIAL OF SERVICE PROTECTION

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

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy. Related control SC-7.

Control Enhancements:

(1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.

(2) The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

LOW SC-5	**MOD** SC-5	**HIGH** SC-5

SC-6 RESOURCE PRIORITY

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

Supplemental Guidance: Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process. This control does not apply to components in the information system for which there is only a single user/role.

Control Enhancements: None.

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

SC-7 BOUNDARY PROTECTION

Control: The information system:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and

b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in an organization-defined security architecture.

Supplemental Guidance: Managed interfaces employing boundary protection devices include, for example, proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in an effective organization-defined security architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Information system boundary protections at designated alternate processing sites provide the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an organizational assessment of risk. FIPS 199 security categorization guides the selection of appropriate candidates for domain partitioning.

The organization carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST Special Publication 800-77 provides guidance on virtual private networks. Related controls: AC-4, IR-4, SC-5.

Control Enhancements:

(1) **The organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces.**

Enhancement Supplemental Guidance: Publicly accessible information system components include, for example, public web servers.

(2) **The information system prevents public access into the organization’s internal networks except as appropriately mediated.**

(3) **The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.**

Enhancement Supplemental Guidance: While this enhancement covers more than just connections to the Internet, the Trusted Internet Connection initiative is an example of limiting the number of managed network access points.

(4) **The organization implements a managed interface for each external telecommunication service, employing security controls as needed to protect the confidentiality and integrity of the information being transmitted.**

(5) **The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).**

(6) **The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.**

(7) The organization prevents the unauthorized exfiltration of information across managed interfaces.

Enhancement Supplemental Guidance: Measures to prevent unauthorized exfiltration of information from the information system include, for example: (i) strict adherence to protocol formats; (ii) monitoring for indications of beaconing from the information system; (iii) monitoring for use of steganography; (iv) disconnecting external network interfaces except when explicitly needed; (v) disassembling and reassembling packet headers; and (vi) employing traffic profile analysis to detect deviations from the volume or types of traffic expected within the organization. Examples of devices enforcing strict adherence to protocol formats include, for example, deep packet inspection firewalls and XML gateways. These devices verify adherence to the protocol specification at the application layer and serve to identify vulnerabilities that cannot be detected by devices operating at the network or transport layer.

(8) The information system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination.

(9) The information system at managed interfaces, denies network traffic and audits internal users (or malicious code) posing a threat to external information systems.

Enhancement Supplemental Guidance: Detecting internal actions that may pose a security threat to external information systems is sometimes termed extrusion detection. Extrusion detection at the information system boundary includes the analysis of network traffic (incoming as well as outgoing) looking for indications of an internal threat to the security of external systems.

(10) The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in non-organization controlled networks.

Enhancement Supplemental Guidance: This enhancement is implemented within the remote device (e.g., notebook computer) via configuration settings that are not configurable by the user of that device. An example of a non-remote communications path from a remote device is an organization-controlled virtual private network (VPN). When a non-remote connection is established via a VPN, the configuration settings prevent what is termed *split-tunneling*. Note that split tunneling might otherwise be used by remote users to communicate with the information system as an extension of that system and to communicate with local resources such as a printer or file server. Since the remote device, when connected by a non-remote connection, becomes an extension of the information system, allowing dual communications paths such as split-tunneling would be, in effect, allowing unauthorized external connections into the system.

(11) The information system routes all internal communications traffic to the Internet through authenticated proxy servers within the managed interfaces of boundary protection devices.

LOW SC-7	**MOD** SC-7 (1) (2) (3) (4) (5) (10)	**HIGH** SC-7 (1) (2) (3) (4) (5) (6) (10) (11)

SC-8 TRANSMISSION INTEGRITY

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

Supplemental Guidance: NIST Special Publication 800-52 provides guidance on protecting transmission integrity using Transport Layer Security (TLS). NIST Special Publication 800-77 provides guidance on protecting transmission integrity using IPsec. NIST Special Publication 800-81 provides guidance on Domain Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems. Related control: AC-17.

Control Enhancements:

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

Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems.

(2) The information system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission.

Enhancement Supplemental Guidance: Information can be intentionally and/or maliciously modified at data aggregation or protocol transformation points, compromising the integrity of the information.

LOW Not Selected	**MOD** SC-8 (1)	**HIGH** SC-8 (1)

SC-9 TRANSMISSION CONFIDENTIALITY

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

Supplemental Guidance: NIST Special Publication 800-52 provides guidance on protecting transmission confidentiality using Transport Layer Security (TLS). NIST Special Publication 800-77 provides guidance on protecting transmission confidentiality using IPsec. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems. Related control: AC-17.

Control Enhancements:

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

Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems.

(2) The information system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.

Enhancement Supplemental Guidance: Information can be intentionally and/or maliciously disclosed at data aggregation or protocol transformation points, compromising the confidentiality of the information.

LOW Not Selected	**MOD** SC-9 (1)	**HIGH** SC-9 (1)

SC-10 NETWORK DISCONNECT

Control: The information system terminates a network connection at the end of a session or after [*Assignment: organization-defined time period*] of inactivity.

Supplemental Guidance: This control applies to both organization-controlled networks and non organization-controlled networks. The organization-defined time period of inactivity may, as the organization deems necessary, be a set of time periods by type of network access or for specific accesses in accordance with an organizational assessment of risk.

Control Enhancements: None.

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

SC-11 TRUSTED PATH

Control: The information system establishes a trusted communications path between the user and the following security functions of the system: [*Assignment: organization-defined security functions to include at a minimum, information system authentication and reauthentication*].

Supplemental Guidance: A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).

Control Enhancements: None.

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

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system.

Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.

Control Enhancements:

(1) The organization maintains availability of information in the event of the loss of cryptographic keys by users.

LOW Not Selected	**MOD** SC-12	**HIGH** SC-12

SC-13 USE OF CRYPTOGRAPHY

Control: The information system implements required cryptographic protections using cryptographic modules that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

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

Control Enhancements: None.

LOW SC-13	**MOD** SC-13	**HIGH** SC-13

SC-14 PUBLIC ACCESS PROTECTIONS

Control: The information system protects the integrity and availability of publicly available information and applications.

Supplemental Guidance: The purpose of this control is to ensure that organizations explicitly consider the protection needs for public information and applications with such protection likely being implemented as part of other security controls.

Control Enhancements: None.

LOW SC-14	**MOD** SC-14	**HIGH** SC-14

SC-15 COLLABORATIVE COMPUTING DEVICES

Control: The information system prohibits remote activation of collaborative computing devices and provides an explicit indication of use to users physically present at the devices.

Supplemental Guidance: Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

Control Enhancements:

(1) **The information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.**

(2) **The information system or supporting environment blocks both inbound and outbound traffic between instant messaging clients that are independently configured by end users and external service providers.**

Enhancement Supplemental Guidance: Blocking restrictions do not include instant messaging services that are configured by an organization to perform an authorized function.

(3) **The organization disables or removes collaborative computing devices from information systems in [*Assignment: organization-defined secure work areas*].**

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

SC-16 TRANSMISSION OF SECURITY PARAMETERS

Control: The information system associates security parameters with information exchanged between information systems.

Supplemental Guidance: Security parameters include, for example, security labels and markings. Security parameters may be explicitly or implicitly associated with the information contained within the information system.

Control Enhancements:

(1) The information system validates the integrity of security parameters exchanged between systems.

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

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control: The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

Supplemental Guidance: For user certificates, each organization either establishes an organizational certification authority cross-certified with the Federal Bridge Certification Authority at medium assurance or higher or uses certificates from an approved, shared service provider, as required by OMB Memorandum 05-24. This control focuses on certificates with a visibility external to the information system and does not include certificates related to internal system operations, for example, application-specific time services. NIST Special Publication 800-32 provides guidance on public key technology. NIST Special Publication 800-63 provides guidance on remote electronic authentication.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-17	**HIGH** SC-17

SC-18 MOBILE CODE

Control: The organization:

a. Establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously;

b. Defines acceptable and unacceptable mobile code; and

c. Authorizes, monitors, and controls the use of mobile code within the information system.

Supplemental Guidance: Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Policy and procedures related to mobile code, address preventing the development, acquisition, or introduction of unacceptable mobile code within the information system. NIST Special Publication 800-28 provides guidance on active content and mobile code.

Control Enhancements: None.

(1) The information system implements detection and inspection mechanisms to identify unauthorized mobile code and takes corrective actions, when necessary.

Enhancement Supplemental Guidance: Corrective actions when unauthorized mobile code is detected include, for example, blocking, quarantine, or alerting administrator.

LOW Not Selected	**MOD** SC-18	**HIGH** SC-18

SC-19 VOICE OVER INTERNET PROTOCOL

Control: The organization:

a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and

b. Authorizes, monitors, and controls the use of VoIP within the information system.

Supplemental Guidance: NIST Special Publication 800-58 provides guidance on security considerations for VoIP technologies employed in information systems.

Control Enhancements: None.

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

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Control: The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.

Supplemental Guidance: This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. The DNS security controls are consistent with, and referenced from, OMB Memorandum 08-23. NIST Special Publication 800-81 provides guidance on secure domain name system deployment.

Control Enhancements:

(1) **The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.**

Enhancement Supplemental Guidance: An example means to indicate the security status of child subspaces is through the use of delegation signer (DS) resource records in the DNS.

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

SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Control: The information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.

Supplemental Guidance: A recursive resolving or caching domain name system (DNS) server is an example of an information system that provides name/address resolution service for local clients. Authoritative DNS servers are examples of authoritative sources. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data. NIST Special Publication 800-81 provides guidance on secure domain name system deployment.

Control Enhancements:

(1) **The information system performs data origin authentication and data integrity verification on all resolution responses whether or not local clients explicitly request this service.**

Enhancement Supplemental Guidance: Local clients include, for example, DNS stub resolvers.

LOW Not Selected	**MOD** Not Selected	**HIGH** SC-21

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

Control: The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement internal/external role separation.

Supplemental Guidance: A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). With regard to role separation, DNS servers with an internal role, only process name/address resolution requests from within the organization (i.e., internal clients). DNS servers with an external role only process name/address resolution information requests from clients external to the organization (i.e., on the public Internet). The set of clients that can access an authoritative DNS server in a particular role is specified by the organization (e.g., by address ranges, explicit lists). NIST Special Publication 800-81 provides guidance on secure DNS deployment.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-22	**HIGH** SC-22

SC-23 SESSION AUTHENTICITY

Control: The information system provides mechanisms to protect the authenticity of communications sessions.

Supplemental Guidance: This control focuses on communications protection at the session, versus packet, level. The intent of this control is to implement session-level protection where needed (e.g., in service-oriented architectures providing web-based services). NIST Special Publication 800-52 provides guidance on the use of transport layer security (TLS) mechanisms. NIST Special Publication 800-77 provides guidance on the deployment of IPsec virtual private networks (VPNs) and other methods of protecting communications sessions. NIST Special Publication 800-95 provides guidance on secure web services.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-23	**HIGH** SC-23

SC-24 FAIL IN KNOWN STATE

Control: The information system fails to a [*Assignment: organization-defined known-state*] for [*Assignment: organization-defined types of failures*].

Supplemental Guidance: Failure in a known state can be interpreted by organizations in the context of safety or security in accordance with the organization’s mission/business/operational needs. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. Failure in a known safe state helps prevent systems from failing to a state that may cause injury to individuals or destruction to property.

Control Enhancements:

(1) The information system preserves [*Assignment: organization-defined system state information*] in failure.

Enhancement Supplemental Guidance: Preserving information system state information facilitates system restart and return to the operational mode of the organization with less disruption of mission/business processes.

LOW Not Selected	**MOD** Not Selected	**HIGH** SC-24

SC-25 THIN NODES

Control: The information system employs processing components that have minimal functionality and data storage.

Supplemental Guidance: The deployment of information system components with minimal functionality (e.g., diskless nodes and thin client technologies), reduces the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to a successful attack.

Control Enhancements: None.

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

SC-26 HONEYPOTS

Control: The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.

Supplemental Guidance: None.

Control Enhancements:

(1) The information system includes components that proactively seek to identify web-based malicious code.

Enhancement Supplemental Guidance: Devices that actively seek out web-based malicious code by posing as clients are referred to as client honeypots or honey clients.

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

SC-27 OPERATING SYSTEM-INDEPENDENT APPLICATIONS

Control: The information system includes [*Assignment: organization-defined operating system-independent applications*].

Supplemental Guidance: Operating system-independent applications are applications that can run on multiple operating systems. Such applications promote portability and reconstitution on different platform architectures, thus increasing the availability for critical functionality while an organization is under an attack exercising vulnerabilities in a given operating system.

Control Enhancements: None.

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

SC-28 CONFIDENTIALITY OF INFORMATION AT REST

Control: The information system protects the confidentiality of information at rest.

Supplemental Guidance: This control is intended to address the confidentiality of information in non-mobile devices.

Control Enhancements:

(1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information at rest unless otherwise protected by alternative physical measures.

LOW Not Selected	**MOD** SC-28	**HIGH** SC-28

SC-29 HETEROGENEITY

Control: The organization employs diverse information technologies in the implementation of the information system.

Supplemental Guidance: Increasing the diversity of information technologies within the information system reduces the impact of from the exploitation of a specific technology.

Control Enhancements: None.

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

SC-30 ABSTRACTION TECHNIQUES

Control: The organization employs abstraction techniques to present information system components as other types of components, or components with differing configurations.

Supplemental Guidance: Abstraction techniques provide organizations with the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms.

Control Enhancements:

(1) The organization employs abstraction techniques to deploy a diversity of operating systems and applications.

Enhancement Supplemental Guidance: Diversity of operating systems and applications may be virtual with the abstraction technique being applied to present what appears to be diversity in the responses at the network interface.

(2) The organization changes the diversity of operating systems and applications [*Assignment: organization-defined frequency*].

Enhancement Supplemental Guidance: While frequent changes to operating systems and applications pose configuration management challenges, the changes result in an increased work-factor for adversaries in order to carry out successful attacks. Changing the apparent operating system or application, as opposed to the actual operating system or application, results in virtual changes that still impede attacker success while helping to reduce the configuration management effort.

(3) The organization employs randomness in the implementation of the abstraction.

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

SC-31 COVERT CHANNEL ANALYSIS

Control: The organization requires that information system developers/integrators perform a covert channel analysis to identify those aspects of system communication that are potential avenues for covert storage and timing channels.

Supplemental Guidance: Information system developers/integrators are in the best position to identify potential avenues within the system that might lead to covert channels. Covert channel analysis is a meaningful activity when there is the potential for unauthorized information flows across security domains, for example, in the case of information systems containing export controlled information and having connections to the Internet.

Control Enhancements:

(1) The organization tests a subset of the vendor identified covert channel avenues to determine if they are exploitable.

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

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates:

a. A formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

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

Control Enhancements: None.

LOW SI-1	**MOD** SI-1	**HIGH** SI-1

SI-2 FLAW REMEDIATION

Control: The organization:

a. Identifies, reports, and corrects information system flaws;

b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and

c. Incorporates flaw remediation into the organizational configuration management process as an emergency change.

Supplemental Guidance: The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously. NIST Special Publication 800-40 provides guidance on security patch installation and patch management. Related controls: CA-2, CA-7, CM-3, MA-2, IR-4, RA-5, SI-11.

Control Enhancements:

(1) The organization centrally manages the flaw remediation process and installs software updates automatically.

Enhancement Supplemental Guidance: Due to information system integrity and availability concerns, organizations should give careful consideration to the methodology used to carry out automatic updates.

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

(3) The organization measures the time between flaw identification and flaw remediation, comparing with organization-defined benchmarks.

(4) The organization employs automated patch management tools to facilitate flaw remediation to [*Assignment: organization-defined information system components*].

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

SI-3 MALICIOUS CODE PROTECTION

Control: The organization:

a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:

- Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
- Inserted through the exploitation of information system vulnerabilities.

b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures;

c. Configures malicious code protection mechanisms to: (i) perform periodic scans of the information system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources as the files are downloaded, opened, or executed; and (ii) disinfect and quarantine infected files;

d. Considers using malicious code protection software products from multiple vendors as part of defense-in-depth; and

e. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Removable media includes, for example, USB devices, diskettes, or compact disks. A variety of technologies exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong software integrity controls may be effective in preventing execution of unauthorized code. Using one vendor for boundary devices and servers and another vendor for workstations is an example of product vendor diversification. NIST Special Publication 800-83 provides guidance on implementing malicious code protection. Related control: SI-4, SI-7.

Control Enhancements:

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

(2) **The information system automatically updates malicious code protection mechanisms (including signature definitions).**

(3) **The information system prevents users from circumventing host-based malicious code protection capabilities.**

(4) **The information system updates malicious code protection mechanisms only when directed by a privileged user.**

(5) **The organization does not allow users to introduce removable media into the information system.**

(6) **The information system implements malicious code protection mechanisms to identify data containing malicious code and responds accordingly (i.e., block, quarantine, send alert to administrator) when the system encounters data not explicitly allowed by the security policy.**

Enhancement Supplemental Guidance: Disallowed transfers include, for example, sending malicious code encoded in various formats (UUENCODE, Unicode) and sending a compressed file containing malicious code.

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

SI-4 INFORMATION SYSTEM MONITORING

Control: The organization:

a. Monitors events on the information system;

b. Detects information system attacks;

c. Identifies unauthorized use of the information system;

d. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;

e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and

f. Consults legal counsel with regard to information system monitoring activities.

Supplemental Guidance: Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, at selected perimeter locations and near server farms supporting critical applications. The granularity of the information collected is determined by the organization based upon its monitoring objectives and the capability of the information system to support such activities. An example of a specific type of transaction of interest to the organization with regard to monitoring is Hyper Text Transfer Protocol (HTTP) traffic that bypasses organizational HTTP proxies, when use of such proxies is required. NIST Special Publication 800-61 provides guidance on detecting attacks through various types of security technologies. NIST Special Publication 800-83 provides guidance on detecting malware-based attacks through malicious code protection software. NIST Special Publication 800-92 provides guidance on monitoring and analyzing computer security event logs. NIST Special Publication 800-94 provides guidance on intrusion detection and prevention. Related controls: AC-8, AU-6, SI-3, SI-7.

Control Enhancements:

(1) The organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.

(2) The organization employs automated tools to support near-real-time analysis of events.

(3) The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

(4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.

Enhancement Supplemental Guidance: Unusual/unauthorized activities or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to an external information system.

(5) The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined list of compromise indicators*].

Enhancement Supplemental Guidance: Alerts may be generated, depending on the organization-defined list of indicators, from a variety of sources, for example, audit records or input from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.

(6) The information system prevents users from circumventing host-based intrusion detection and prevention capabilities.

(7) The information system notifies [*Assignment: organization-defined list of incident response personnel*] of suspicious events and takes [*Assignment: organization-defined list of least-disruptive actions to terminate suspicious events*].

Enhancement Supplemental Guidance: The least-disruptive actions may include initiating request for human response.

(8) The organization protects information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion.

(9) The organization tests/exercises intrusion monitoring tools [*Assignment: organization-defined time-period*].

Enhancement Supplemental Guidance: The frequency of testing/exercises is dependent upon the type and method of deployment of the intrusion monitoring tools.

(10) The organization makes provisions so that encrypted traffic is visible to information system monitoring tools.

Enhancement Supplemental Guidance: The enhancement recognizes the need to balance encrypting traffic versus the need to have insight into that traffic from a monitoring perspective. For some organizations, the need to ensure the confidentiality of traffic is paramount, for others the mission assurance concerns are greater.

(11) The information system analyzes outbound communications traffic at the external boundary of the system (i.e., system perimeter) and, as deemed necessary, at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies.

Enhancement Supplemental Guidance: Anomalies within the information system include, for example, large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.

LOW Not Selected	**MOD** SI-4 (2) (4) (5) (6)	**HIGH** SI-4 (2) (4) (5) (6)

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Control: The organization:

a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;

b. Generates internal security alerts, advisories, and directives as deemed necessary;

c. Disseminates security alerts, advisories, and directives to [*Assignment: organization-defined list of personnel*]; and

d. Implements security directives in accordance with timeframes established by the directives, or notifies the issuing organization of the degree of non-compliance.

Supplemental Guidance: Security alerts and advisories are generated by the United States Computer Emergency Readiness Team (US-CERT) to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organization with the responsibility and authority to issue such directives. Compliance to security directives is *essential* due to the critical nature of many of these directives and the potential immediate adverse affects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner. NIST Special Publication 800-40 provides guidance on monitoring and distributing security alerts and advisories.

Control Enhancements:

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

LOW SI-5	**MOD** SI-5	**HIGH** SI-5 (1)

SI-6 SECURITY FUNCTIONALITY VERIFICATION

Control: The information system verifies the correct operation of security functions [*Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every* [*Assignment: organization-defined time-period*]] and [*Selection (one or more): notifies system administrator, shuts the system down, restarts the system*] when anomalies are discovered.

Supplemental Guidance: The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required.

Control Enhancements:

(1) The information system provides notification of failed automated security tests.

(2) The information system provides automated support for the management of distributed security testing.

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

SI-7 SOFTWARE AND INFORMATION INTEGRITY

Control: The information system detects unauthorized changes to software and information.

Supplemental Guidance: The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.

Control Enhancements:

(1) The organization reassesses the integrity of software and information by performing [*Assignment: organization-defined frequency*] integrity scans of the information system.

(2) The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.

(3) The organization employs centrally managed integrity verification tools.

(4) The organization requires use of tamper evident packaging for [*Assignment: organization-defined information system components*] during [*Selection: transportation from vendor to operational site, during operation, both*].

LOW Not Selected	**MOD** Not Selected	**HIGH** SI-7 (1) (2)

SI-8 SPAM PROTECTION

Control: The organization:

a. Employs spam protection mechanisms at information system entry points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means;

b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures; and

c. Considers using spam protection software products from multiple vendors as part of defense-in-depth.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Using one vendor for boundary devices and servers and another vendor for workstations is an example of product vendor diversification. NIST Special Publication 800-45 provides guidance on electronic mail security.

Control Enhancements:

(1) The organization centrally manages spam protection mechanisms.

(2) The information system automatically updates spam protection mechanisms (including signature definitions).

LOW Not Selected	**MOD** SI-8	**HIGH** SI-8 (1)

SI-9 INFORMATION INPUT RESTRICTIONS

Control: The organization restricts the capability to input information to the information system to authorized personnel.

Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

Control Enhancements: None.

LOW Not Selected	**MOD** SI-9	**HIGH** SI-9

SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY

Control: The information system checks information for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.

Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.

Control Enhancements: None.

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

SI-11 ERROR HANDLING

Control: The information system:

a. Identifies error conditions;

b. Generates error messages that provide information necessary for corrective actions without revealing potentially harmful information that could be exploited by adversaries;

c. Reveals error messages only to authorized personnel; and

d. Prohibits inclusion of sensitive information in error logs or associated administrative messages.

Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. Sensitive information includes, for example, account numbers, social security numbers, and credit card numbers.

Control Enhancements: None.

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

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION

Control: The organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Supplemental Guidance: The National Archives and Records Administration provides guidance on records retention. Related controls: MP-2, MP-4.

Control Enhancements: None.

LOW Not Selected	**MOD** SI-12	**HIGH** SI-12

SI-13 PREDICTABLE FAILURE PREVENTION

Control: The organization:

a. Protects the information system from harm by considering mean time to failure for [*Assignment: organization-defined list of information system components*] in specific environments of operation; and

b. Provides substitute information system components, when needed, and a mechanism to exchange active and standby roles of the components.

Supplemental Guidance: Mean time to failure rates are defendable and based on considerations that are installation-specific, not industry average. The transfer of responsibilities between active and standby information system components does not compromise safety, operational readiness, or security (e.g., state variables are preserved). The standby component is available at all times except where a failure recovery is in progress, or for maintenance reasons.

Control Enhancements:

(1) The organization takes the information system component out of service by transferring component responsibilities to a substitute component no later than [*Assignment: organization-defined fraction or percentage*] of mean time to failure.

(2) The organization does not allow a process to execute without supervision for more than [*Assignment: organization-defined time period*].

(3) The organization manually initiates a transfer between active and standby information system components at least once per [*Assignment: organization-defined frequency*] if the mean time to failure exceeds [*Assignment: organization-defined time period*].

(4) The organization, if an information system component failure is detected:

(a) Ensures that the standby information system component successfully and transparently assumes its role within [*Assignment: organization-defined time period*]; and

(b) [*Selection: activates* [*Assignment: organization-defined alarm*] *and/or automatically shuts down the information system*].

Enhancement Supplemental Guidance: Automatic or manual transfer of roles to a standby unit may occur upon detection of a component failure.

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

APPENDIX G

INFORMATION SECURITY PROGRAMS

ORGANIZATION-WIDE INFORMATION SECURITY PROGRAM MANAGEMENT CONTROLS

The Federal Information Security Management Act (FISMA) requires organizations to develop and implement an organization-wide information security program to address information security for the information and information systems that support the operations and assets of the organization, including those provided or managed by another organization, contractor, or other source. The information security program management (PM) controls described in this Appendix, complement the security controls in Appendix F and focus on the organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs. Organizations document program management controls in an organization-wide *information security program plan*. The organization-wide security program plan supplements the individual security plans developed for each organizational information system. Together, the security plans for the individual information systems and the security plan for the information security program cover the totality of security controls employed by the organization.

In addition to documenting the information security program management controls, the security program plan provides a vehicle for the organization to document in a central repository, all security controls from Appendix F that have been designated as *common controls* (i.e., security controls inherited by organizational information systems). The program management controls and common controls contained in the information security program plan should be implemented, assessed for effectiveness,[51] and approved/authorized for use by a senior organizational official, with the same or similar authority and responsibility for managing risk as the authorization officials for information systems.[52] Plans of action and milestones are developed and maintained for the program management and common controls that are deemed through assessment, to be less than effective. Program management and common controls are also subject to the same continuous monitoring requirements as security controls employed in individual organizational information systems.

[51] Assessment procedures for program management controls and common controls can be found in NIST Special Publication 800-53A.

[52] In situations where common controls are inherited from external environments, organizations should consult the guidance provided in Section 3.4.

PM-1 SECURITY PROGRAM PLAN

Control: The organization:

a. Develops and disseminates an organization-wide information security program plan that:

- Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
- Provides sufficient information about the program management controls and common controls (including specification of parameters for any *assignment* and *selection* operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;
- Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
- Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;

b. Reviews the organization-wide security program plan [*Assignment: organization-defined frequency, at least annually*]; and

c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.

Supplemental Guidance: The information security program plan documents the organization-wide program management controls and organization-defined common controls. The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls.

Organizations have the flexibility to describe common controls in a separate document or multiple documents in situations where different organizational entities are assigned responsibility and are accountable for the implementation, assessment, and approval of the common controls that are not implemented as part of an information system. In those cases, the documents describing common controls are included as attachments to the information security program plan. If multiple common control documents are contained in the information security program plan, the organization specifies in each document, the organizational official or officials responsible for the implementation, assessment, and approval of the common controls included in the respective documents. For example, the organization may require that the Facilities Management Office develop, implement, assess, and approve common physical and environmental protection controls or that the Human Resources Office develop, implement, assess, and approve common personnel security controls when such controls are not associated with an information system.

Control Enhancements: None.

PM-2 SENIOR AGENCY INFORMATION SECURITY OFFICER

Control: The organization appoints a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Supplemental Guidance: The security officer described in this control is an official of a federal agency (as defined in applicable laws, Executive Orders, directives, policies, or regulations) or an official of an appropriate subordinate organization of a federal agency. Organizations may also refer to this organizational official as the Senior Information Security Officer or Chief Information Security Officer.

Control Enhancements: None.

PM-3 INFORMATION SECURITY RESOURCES

Control: The organization:

a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;

b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and

c. Ensures that information security resources are available for expenditure as planned.

Supplemental Guidance: Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process. NIST Special Publication 800-65 provides guidance on integrating security into the capital planning and investment control process.

Control Enhancements: None.

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

Control: The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions (from identification of needed action through assessment of implementation) to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.

Supplemental Guidance: The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones.

Control Enhancements: None.

PM-5 INFORMATION SYSTEM INVENTORY

Control: The organization develops and maintains an inventory of its information systems.

Supplemental Guidance: This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements.

Control Enhancements: None.

PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE

Control: The organization develops, monitors, and reports on the results of information security measures of performance.

Supplemental Guidance: Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program. NIST Special Publication 800-55 provides guidance on performance measures for information security.

Control Enhancements: None.

PM-7 ENTERPRISE ARCHITECTURE

Control: The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

Supplemental Guidance: The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. Security requirements and control integration are most effectively accomplished through the application of the Risk Management Framework and supporting NIST standards and guidelines. The Federal Enterprise Architecture Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures. NIST Special Publication 800-39 provides guidance on managing risk from information systems from a security life cycle perspective. Related controls: PM-11, RA-2.

Control Enhancements: None.

PM-8 CRITICAL INFRASTRUCTURE PLAN

Control: The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Supplemental Guidance: The critical infrastructure and key resources protection plan is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Control Enhancements: None.

PM-9 RISK MANAGEMENT STRATEGY

Control: The organization:

a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and

b. Implements that strategy consistently across the organization.

Supplemental Guidance: An organization-wide risk management strategy should include, for example, an unambiguous expression of the risk tolerance of the organization, guidance on acceptable risk assessment methodologies, and a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. NIST Special Publication 800-39 provides guidance on managing risk from information systems.

Control Enhancements: None.

PM-10 SECURITY AUTHORIZATION PROCESS

Control: The organization:

a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; and

b. Fully integrates the security authorization processes into an organization-wide risk management strategy.

Supplemental Guidance: The security authorization process for information systems requires the implementation of the Risk Management Framework and the employment of associated security standards and guidelines.

Control Enhancements: None.

PM-11 MISSION/BUSINESS PROCESS DEFINITION

Control: The organization:

a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and

b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.

Supplemental Guidance: Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Inherent in defining an organization's information protection needs is an understanding of the level of adverse impact that could result if a compromise occurs, and hence a categorization of information in accordance with FIPS 199 and NIST Special Publication 800-60. Modeling and simulation techniques can help in discerning the security ramification in mission/business process definitions. Related controls: PM-8, RA-2.

Control Enhancements: None.

TABLE G-1: PROGRAM MANAGEMENT CONTROLS

CONTROL NUMBER	CONTROL NAME	TARGET DELOYMENT
PM-1	Security Program Plan	Organization-level Application
PM-2	Senior Agency Information Security Officer	Organization-level Application
PM-3	Information Security Resources	Organization-level Application
PM-4	Plan of Action and Milestones Process	Organization-level Application
PM-5	Information System Inventory	Organization-level Application
PM-6	Information Security Measures of Performance	Organization-level Application
PM-7	Enterprise Architecture	Organization-level Application
PM-8	Critical Infrastructure Plan	Organization-level Application
PM-9	Risk Management Strategy	Organization-level Application
PM-10	Security Authorization Process	Organization-level Application
PM-11	Mission/Business Process Definition	Organization-level Application

APPENDIX H

INTERNATIONAL INFORMATION SECURITY STANDARDS

SECURITY CONTROL MAPPINGS FOR ISO/IEC 27001

The mapping tables in this appendix provides organizations with a *general* indication of security control coverage with respect to ISO/IEC 27001, *Information technology–Security techniques–Information security management systems–Requirements*.[53] ISO/IEC 27001 applies to all types of organizations (e.g. commercial, government) and specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system (ISMS) within the context of the organization's overall business risks. While the risk management approach established by NIST originally focused on managing risk from information systems (as required by FISMA and described in NIST Special Publication 800-39), the approach is being expanded to include risk management at the organizational level. A forth-coming version of NIST Special Publication 800-39 will incorporate ISO/IEC 27001 to manage organizational information security risk through the establishment of an ISMS. Since NIST's mission includes the adoption of international and national standards where appropriate, NIST intends to pursue convergence to reduce the burden on organizations that must conform to both sets of standards. The convergence initiative will be carried out in three phases. Phase I, the subject of this Appendix, provides a two-way mapping between the security controls in NIST Special Publication 800-53 and the controls in ISO/IEC 27001 (Annex A). Phase II will provide a two-way mapping between the organization-level risk management concepts in NIST Special Publication 800-39 (forth-coming version) and general requirements in ISO/IEC 27001. Phase III will use the results from Phase I and II to fully integrate ISO/IEC 27001 into NIST's risk management approach such that an organization that complies with NIST standards and guidelines can also comply with ISO/IEC 27001 (subject to appropriate assessment requirements for ISO/IEC 27001 certification).

Table H-1 provides a forward mapping from the security controls in NIST Special Publication 800-53 to the controls in ISO/IEC 27001 (Annex A). The mappings are created by using the primary security topic identified in each of the Special Publication 800-53 security controls and associated control enhancements (if any) and searching for a similar security topic in ISO/IEC 27001 (Annex A). Security controls with similar functional meaning are included in the mapping table. For example, Special Publication 800-53 contingency planning and ISO/IEC 27001 (Annex A) business continuity were deemed to have similar, but not the same, functionality. In some cases, similar topics are addressed in the security control sets but provide a different context, perspective, or scope. For example, Special Publication 800-53 addresses information flow control broadly in terms of assigned authorizations for controlling access between source and destination objects, whereas ISO/IEC 27001 (Annex A) addresses the information flow more narrowly as it applies to interconnected network domains. Table H-2 provides a reverse mapping from the security controls in Special Publication 800-53 to the security controls in ISO/IEC 27001 (Annex A).[54]

[53] ISO/IEC 27001 was published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

[54] The use of the term *XX-1 controls* in mapping Table H-2 refers to the set of security controls represented by the first control in each family in NIST Special Publication 800-53, where *XX* is a placeholder for the two-letter family identifier. These security controls primarily focus on policies and procedures for each topic area addressed by the respective security control family.

Organizations are encouraged to use the mapping tables as a starting point for conducting further analyses and interpretation of the extent of compliance with ISO/IEC 27001 from compliance with the NIST security standards and guidelines and visa versa. Organizations that use the security controls in Special Publication 800-53 as an extension to the security controls in Annex A in their ISO/IEC 27001 implementations will have a higher probability of complying with NIST security standards and guidelines than those organizations that use only Annex A.

TABLE H-1: MAPPING NIST SP 800-53 TO ISO/IEC 27001 (ANNEX A)

NIST SP 800-53 CONTROLS		ISO/IEC 27001 (Annex A) CONTROLS
AC-1	Access Control Policy and Procedures	A5.1.1, A5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A10.1.1, A.10.8.1, A.11.1.1, A.11.2.1, A11.2.2, A11.4.1, A.11.7.1, A.11.7.2, A.15.1.1, A.15.2.1
AC-2	Account Management	A.8.3.3, A.11.2.1, A.11.2.2, A.11.2.4, A15.2.1
AC-3	Access Enforcement	A.10.8.1 A.11.4.4, A.11.4.6, A.11.5.4, A.11.6.1, A.12.4.2
AC-4	Information Flow Enforcement	A.10.6.1, A.10.8.1, A.11.4.5, A.11.4.7, A.11.7.2, A.12.4.2, A.12.5.4
AC-5	Separation of Duties	A.6.1.3, A.8.1.1, A.10.1.3, A.11.1.1, A.11.4.1
AC-6	Least Privilege	A.6.1.3, A.8.1.1, A.11.1.1, A.11.2.2, A.11.4.1, A.11.4.4, A.11.4.6, A.11.5.4, A.11.6.1, A.12.4.3
AC-7	Unsuccessful Login Attempts	A.11.5.1
AC-8	System Use Notification	A.6.2.2, A.8.1.1, A.11.5.1, A.15.1.5
AC-9	Previous Logon Notification	A.11.5.1
AC-10	Concurrent Session Control	A.11.5.1
AC-11	Session Lock	A.11.3.2, A.11.3.3, A.11.5.5
AC-12	**Withdrawn**	---
AC-13	**Withdrawn**	---
AC-14	Permitted Actions without Identification or Authentication	A.11.6.1
AC-15	**Withdrawn**	---
AC-16	Automated Labeling	A.7.2.2
AC-17	Remote Access	A.10.6.1, A.10.8.1, A.11.1.1, A.11.4.1, A.11.4.2, A.11.4.4, A.11.4.6, A.11.4.7, A.11.7.1, A.11.7.2
AC-18	**Withdrawn**	---
AC-19	Access Control for Mobile Devices	A.10.4.1, A.11.1.1, A.11.4.3, A.11.7.1
AC-20	Use of External Information Systems	A.7.1.3, A.8.1.1, A.8.1.3, A.10.6.1, A.10.8.1, A.11.4.1, A.11.4.2
AC-21	User-based Collaboration and Information Sharing	A.11.2.1, A.11.2.2
AT-1	Security Awareness and Training Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
AT-2	Security Awareness	A.6.2.2, A.8.1.1, A.8.2.2, A.9.1.5, A.10.4.1
AT-3	Security Training	A.8.1.1, A.8.2.2, A.9.1.5
AT-4	Security Training Records	None
AT-5	Contacts with Security Groups and Associations	A.6.1.7
AU-1	Audit and Accountability Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.10.10.2, A.15.1.1, A.15.2.1, A.15.3.1
AU-2	Auditable Events	A.10.10.1, A.10.10.4, A.10.10.5, A.15.3.1
AU-3	Content of Audit Records	A.10.10.1
AU-4	Audit Storage Capacity	A.10.10.1, A.10.3.1
AU-5	Response to Audit Processing Failures	A.10.3.1, A.10.10.1
AU-6	Audit Review, Analysis, and Reporting	A.10.10.2, A.10.10.5, A.13.1.1, A.15.1.5
AU-7	Audit Reduction and Report Generation	A.10.10.2
AU-8	Time Stamps	A.10.10.1, A.10.10.6
AU-9	Protection of Audit Information	A.10.10.3, A.13.2.3, A.15.1.3, A.15.3.2
AU-10	Non-repudiation	A.10.9.1, A.12.2.3
AU-11	Audit Record Retention	A.10.10.1, A.10.10.2, A.15.1.3
AU-12	Audit Generation	A.10.10.1, A.10.10.4, A.10.10.5
CA-1	Security Assessment and Authorization Policies and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3 A.6.1.4, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
CA-2	Security Assessments	A.6.1.8, A.10.3.2, A.15.2.1, A.15.2.2
CA-3	Information System Connections	A.6.2.1, A.6.2.3, A.10.6.1, A.10.8.1, A.10.8.2, A.10.8.5, A.11.4.2
CA-4	**Withdrawn**	---
CA-5	Plan of Action and Milestones	None
CA-6	Security Authorization	A.6.1.4, A.10.3.2
CA-7	Continuous Monitoring	A.6.1.8, A.15.2.1, A.15.2.2

NIST SP 800-53 CONTROLS		ISO/IEC 27001 (Annex A) CONTROLS
CM-1	Configuration Management Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.10.1.2, A.12.4.1, A.12.5.1, A.15.1.1, A.15.2.1
CM-2	Baseline Configuration	A.12.4.1, A.10.1.4
CM-3	Configuration Change Control	A.10.1.1, A.10.1.2, A.10.3.2, A.12.4.1, A.12.5.1, A.12.5.2, A.12.5.3
CM-4	Security Impact Analysis	A.10.1.2, A.10.3.2, A.12.4.1, A.12.5.2, A.12.5.3
CM-5	Access Restrictions for Change	A.10.1.2, A.11.1.1, A.11.6.1, A.12.4.1, A.12.4.3, A.12.5.3
CM-6	Configuration Settings	None
CM-7	Least Functionality	None
CM-8	Information System Component Inventory	A.7.1.1, A.7.1.2
CM-9	Configuration Management Plan	A.6.1.3. A.7.1.1, A.7.1.2, A.8.1.1, A.10.1.1, A.10.1.2, A.10.3.2, A.12.4.1, A.12.4.3, A.12.5.1, A.12.5.2, A.12.5.3
CP-1	Contingency Planning Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.9.1.4, A.10.1.1, A.10.1.2, A.14.1.1, A.14.1.3, A.15.1.1, A.15.2.1
CP-2	Contingency Plan	A.6.1.2, A.9.1.4, A.10.3.1, A.14.1.1, A.14.1.2, A.14.1.3, A.14.1.4, A.14.1.5
CP-3	Contingency Training	A.8.2.2, A.9.1.4, A.14.1.3
CP-4	Contingency Plan Testing and Exercises	A.6.1.2, A.9.1.4, A.14.1.1, A.14.1.3, A.14.1.4, A.14.1.5
CP-5	**Withdrawn**	---
CP-6	Alternate Storage Site	A.9.1.4, A.14.1.3
CP-7	Alternate Processing Site	A.9.1.4, A.14.1.3
CP-8	Telecommunications Services	A.9.1.4, A.10.6.1, A.14.1.3
CP-9	Information System Backup	A.9.1.4, A.10.5.1, A.14.1.3, A.15.1.3
CP-10	Information System Recovery and Reconstitution	A.9.1.4, A.14.1.3
IA-1	Identification and Authentication Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.11.2.1, A.15.1.1, A.15.2.1
IA-2	Identification and Authentication (Organizational Users)	A.11.3.2, A.11.5.1, A.11.5.2, A.11.5.3
IA-3	Device Identification and Authentication	A.11.4.3
IA-4	Identifier Management	A.11.5.2
IA-5	Authenticator Management	A.11.2.1, A.11.2.3, A.11.3.1, A.11.5.2, A.11.5.3
IA-6	Authenticator Feedback	A.11.5.1
IA-7	Cryptographic Module Authentication	A.12.3.1, A.15.1.1, A.15.1.6, A.15.2.1
IA-8	Identification and Authentication (Non Organizational Users)	A.10.9.1, A.11.4.2, A.11.5.1, A.11.5.2
IR-1	Incident Response Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.13.1.1, A.13.2.1, A.15.1.1, A.15.2.1
IR-2	Incident Response Training	A.8.2.2
IR-3	Incident Response Testing and Exercises	None
IR-4	Incident Handling	A.6.1.2, A.13.2.2, A.13.2.3
IR-5	Incident Monitoring	None
IR-6	Incident Reporting	A.6.1.6, A.13.1.1
IR-7	Incident Response Assistance	None
MA-1	System Maintenance Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.9.2.4, A.10.1.1, A.15.1.1, A.15.2.1
MA-2	Controlled Maintenance	A.9.2.4
MA-3	Maintenance Tools	A.9.2.4, A.11.4.4
MA-4	Remote Maintenance	A.9.2.4, A.11.4.4
MA-5	Maintenance Personnel	A.9.2.4, A.12.4.3
MA-6	Timely Maintenance	A.9.2.4
MP-1	Media Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.10.7.1, A.10.7.2, A.10.7.3, A.11.1.1, A.15.1.1, A.15.1.3, A.15.2.1
MP-2	Media Access	A.7.2.2, A.10.7.1, A.10.7.3
MP-3	Media Marking	A.7.2.2, A.10.7.1, A.10.7.3
MP-4	Media Storage	A.10.7.1, A.10.7.3, A.10.7.4, A.15.1.3
MP-5	Media Transport	A.9.2.5, A.9.2.7, A.10.7.1, A.10.7.3, A.10.8.3
MP-6	Media Sanitization	A.9.2.6, A.10.7.1, A.10.7.2, A.10.7.3

NIST SP 800-53 CONTROLS		ISO/IEC 27001 (Annex A) CONTROLS
PE-1	Physical and Environmental Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.9.1.4, A.9.2.1, A.9.2.2, A.10.1.1, A.11.1.1, A.11.2.1, A.11.2.2, A.15.1.1, A.15.2.1
PE-2	Physical Access Authorizations	A.9.1.5, A.11.2.1, A.11.2.2, A.11.2.4
PE-3	Physical Access Control	A.9.1.1, A.9.1.2, A.9.1.3, A.9.1.5, A.9.1.6, A.11.3.2, A.11.4.4
PE-4	Access Control for Transmission Medium	A.9.1.3, A.9.1.5, A.9.2.3
PE-5	Access Control for Display Medium	A.9.1.2, A.9.1.3, A.10.6.1, A.11.3.2
PE-6	Monitoring Physical Access	A.9.1.2, A.9.1.5, A.10.10.2
PE-7	Visitor Control	A.9.1.2, A.9.1.5, A.9.1.6
PE-8	Access Records	A.9.1.5, A.10.10.2, A.15.2.1
PE-9	Power Equipment and Power Cabling	A.9.1.4, A.9.2.2, A.9.2.3
PE-10	Emergency Shutoff	A.9.1.4
PE-11	Emergency Power	A.9.1.4, A.9.2.2
PE-12	Emergency Lighting	A.9.2.2
PE-13	Fire Protection	A.9.1.4
PE-14	Temperature and Humidity Controls	A.9.2.2
PE-15	Water Damage Protection	A.9.1.4
PE-16	Delivery and Removal	A.9.1.6, A.9.2.7, A.10.7.1
PE-17	Alternate Work Site	A.9.2.5, A.11.7.2
PE-18	Location of Information System Components	A.9.2.1, A.11.3.2
PE-19	Information Leakage	A.12.5.4
PL-1	Security Planning Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
PL-2	System Security Plan	None
PL-3	**Withdrawn**	---
PL-4	Rules of Behavior	A.6.1.5, A.6.2.2, A.7.1.3. A.8.1.1, A.8.1.3, A.8.2.1, A.9.1.5, A.10.8.1, A.11.7.1, A.11.7.2, A.12.4.1, A.13.1.2, A.15.1.5
PL-5	Privacy Impact Assessment	A.15.1.4
PL-6	Security-Related Activity Planning	A.6.1.2, A.15.3.1
PM-1	Security Program Plan	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3 A.8.1.1, A.15.1.1, A.15.2.1
PM-2	Senior Agency Information Security Officer	A.6.1.1, A.6.1.2, A.6.1.3
PM-3	Information Security Resources	None
PM-4	Plan of Action and Milestones Process	None
PM-5	Information System Inventory	A.7.1.1, A.7.1.2
PM-6	Information Security Measures of Performance	None
PM-7	Enterprise Architecture	None
PM-8	Critical Infrastructure Plan	None
PM-9	Risk Management Strategy	A.6.2.1, A.14.1.2
PM-10	Security Authorization Process	A.6.1.4
PM-11	Mission/Business Process Definition	None
PS-1	Personnel Security Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
PS-2	Position Categorization	A.8.1.1
PS-3	Personnel Screening	A.8.1.2
PS-4	Personnel Termination	A.8.3.1, A.8.3.2, A.8.3.3
PS-5	Personnel Transfer	A.8.3.1, A.8.3.2, A.8.3.3
PS-6	Access Agreements	A.6.1.5, A.8.1.1, A.8.1.3, A.8.2.1, A.9.1.5, A.10.8.1, A.11.7.1, A.11.7.2, A.15.1.5
PS-7	Third-Party Personnel Security	A.6.2.3, A.8.1.1, A.8.2.1, A.8.1.3
PS-8	Personnel Sanctions	A.8.2.3, A.15.1.5
RA-1	Risk Assessment Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.14.1.2, A.15.1.1, A.15.2.1
RA-2	Security Categorization	A.7.2.1, A.14.1.2
RA-3	Risk Assessment	A.6.2.1, A.10.2.3, A.12.6.1, A.14.1.2
RA-4	**Withdrawn**	---
RA-5	Vulnerability Scanning	A.12.6.1, A.15.2.2
SA-1	System and Services Acquisition Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.6.2.1, A.8.1.1, A.10.1.1, A.12.1.1, A.12.5.5, A.15.1.1, A.15.2.1

NIST SP 800-53 CONTROLS		ISO/IEC 27001 (Annex A) CONTROLS
SA-2	Allocation of Resources	A.6.1.2, A.10.3.1
SA-3	Life Cycle Support	A.12.1.1
SA-4	Acquisitions	A.12.1.1, A.12.5.5
SA-5	Information System Documentation	A.10.7.4, A.15.1.3
SA-6	Software Usage Restrictions	A.12.4.1, A.12.5.5, A.15.1.2
SA-7	User Installed Software	A.12.4.1, A.12.5.5, A.15.1.5
SA-8	Security Engineering Principles	A.10.4.1, A.10.4.2, A.11.4.5, A.12.5.5
SA-9	External Information System Services	A.6.1.5, A.6.2.1, A.6.2.3, A.8.1.1, A.8.2.1, A.10.2.1, A.10.2.2, A.10.2.3, A.10.6.2, A.10.8.2, A.12.5.5
SA-10	Developer Configuration Management	A.12.4.3, A.12.5.1, A.12.5.5
SA-11	Developer Security Testing	A.10.3.2, A.12.5.5
SA-12	Supply Chain Protections	A.12.5.5
SA-13	Trustworthiness	A.12.5.5
SC-1	System and Communications Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
SC-2	Application Partitioning	A.10.4.1, A.10.4.2
SC-3	Security Function Isolation	A.10.4.1, A.10.4.2, A.10.9.1, A.10.9.2
SC-4	Information In Shared Resources	None
SC-5	Denial of Service Protection	A.10.3.1
SC-6	Resource Priority	None
SC-7	Boundary Protection	A.6.2.1, A.10.4.1, A.10.4.2, A.10.6.1, A.10.8.1, A.10.9.1, A.10.9.2, A.10.10.2, A.11.4.5, A.11.4.6
SC-8	Transmission Integrity	A.10.4.2, A.10.6.1, A.10.6.2, A.10.9.1, A.10.9.2, A.12.2.3, A.12.3.1
SC-9	Transmission Confidentiality	A.10.6.1, A.10.6.2, A.10.9.1, A.10.9.2, A.12.3.1
SC-10	Network Disconnect	A.10.6.1, A.11.3.2, A.11.5.1, A.11.5.5
SC-11	Trusted Path	None
SC-12	Cryptographic Key Establishment and Management	A.12.3.2
SC-13	Use of Cryptography	A.12.3.1, A.15.1.6
SC-14	Public Access Protections	A.10.4.1, A.10.4.2, A.10.9.1, A.10.9.2, A.10.9.3
SC-15	Collaborative Computing Devices	None
SC-16	Transmission of Security Parameters	A.7.2.2, A.10.8.1
SC-17	Public Key Infrastructure Certificates	A.12.3.2
SC-18	Mobile Code	A.10.4.2
SC-19	Voice Over Internet Protocol	A.10.6.1
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	A.10.6.1
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	A.10.6.1
SC-22	Architecture and Provisioning for Name/Address Resolution Service	A.10.6.1
SC-23	Session Authenticity	A.10.6.1
SC-24	Fail in Known State	None
SC-25	Thin Nodes	None
SC-26	Honeypots	None
SC-27	Operating System-Independent Applications	None
SC-28	Confidentiality of Information at Rest	None
SC-29	Heterogeneity	None
SC-30	Abstraction Techniques	None
SC-31	Covert Channel Analysis	None
SI-1	System and Information Integrity Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
SI-2	Flaw Remediation	A.10.10.5, A.12.5.2, A.12.6.1, A.13.1.2
SI-3	Malicious Code Protection	A.10.4.1
SI-4	Information System Monitoring	A.10.10.2, A.13.1.1, A.13.1.2
SI-5	Security Alerts, Advisories, and Directives	A.6.1.6, A.12.6.1, A.13.1.1, A.13.1.2
SI-6	Security Functionality Verification	None
SI-7	Software and Information Integrity	A.10.4.1, A.12.2.2, A.12.2.3

NIST SP 800-53 CONTROLS		ISO/IEC 27001 (Annex A) CONTROLS
SI-8	Spam Protection	None
SI-9	Information Input Restrictions	A.10.8.1, A.11.1.1, A.11.2.2, A.12.2.2
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	A.12.2.1, A.12.2.2
SI-11	Error Handling	None
SI-12	Information Output Handling and Retention	A.10.7.3, A.15.1.3, A.15.1.4, A.15.2.1
SI-13	Predictable Failure Prevention	None

TABLE H-2: MAPPING ISO/IEC 27001 (ANNEX A) TO NIST SP 800-53

ISO/IEC 27001 (Annex A) CONTROLS	NIST SP 800-53 CONTROLS
A.5 Security Policy	
A.5.1 Information security policy	
A.5.1.1 Information security policy document	XX-1 controls
A.5.1.2 Review of the information security policy	XX-1 controls
A.6 Organization of information security	
A.6.1 Internal	
A.6.1.1 Management commitment to information security	XX-1 controls, PM-2; SP 800-39, SP 800-37
A.6.1.2 Information security coordination	CP-2, CP-4, IR-4, PL-1, PL-6, PM-2, SA-2; SP 800-39, SP 800-37
A.6.1.3 Allocation of information security responsibilities	XX-1 controls, AC-5, AC-6, CM-9. PM-2; SP 800-39, SP 800-37
A.6.1.4 Authorization process for information processing facilities	CA-1, CA-6, PM-10; SP 800-37
A.6.1.5 Confidentiality agreements	PL-4, PS-6, SA-9
A.6.1.6 Contact with authorities	Multiple controls with contact reference (e.g., IR-6, SI-5); SP 800-39; SP 800-37
A.6.1.7 Contact with special interest groups	AT-5
A.6.1.8 Independent review of information security	CA-2, CA-7; SP 800-39, SP 800-37
A.6.2 External Parties	
A.6.2.1 Identification of risks related to external parties	CA-3, PM-9, RA-3, SA-1, SA-9, SC-7
A.6.2.2 Addressing security when dealing with customers	AC-8 , AT-2, PL-4
A.6.2.3 Addressing security in third party agreements	CA-3, PS-7, SA-9
A.7 Asset Management	
A.7.1 Responsibility for assets	
A.7.1.1 Inventory of assets	CM-8, CM-9, PM-5
A.7.1.2 Ownership of assets	CM-8, CM-9, PM-5
A.7.1.3 Acceptable use of assets	AC-20, PL-4
A.7.2 Information Classification	
A.7.2.1 Classification Guidelines	RA-2
A.7.2.2 Information labeling and handling	AC-16, MP-2, MP-3, SC-16
A.8 Human Resources Security	
A.8.1 Prior to Employment	
A.8.1.1 Roles and Responsibilities	XX-1 controls, AC-5, AC-6, AC-8, AC-20, AT-2, AT-3, CM-9, PL-4, PS-2, PS-6, PS-7, SA-9
A.8.1.2 Screening	PS-3
A.8.1.3 Terms and conditions of employment	AC-20, PL-4, PS-6, PS-7
A.8.2 During employment	
A.8.2.1 Management responsibilities	PL-4, PS-6, PS-7, SA-9
A.8.2.2 Awareness, education, and training	AT-2, AT-3, IR-2
A.8.2.3 Disciplinary process	PS-8
A.8.3 Termination or change of employment	
A.8.3.1 Termination responsibilities	PS-4, PS-5
A.8.3.2 Return of assets	PS-4, PS-5
A.8.3.3 Removal of access rights	AC-2, PS-4, PS-5
A.9 Physical and environmental security	
A.9.1 Secure areas	
A.9.1.1 Physical security perimeter	PE-3
A.9.1.2 Physical entry controls	PE-3, PE-5, PE-6, PE-7
A.9.1.3 Securing offices, rooms, facilities	PE-3, PE-4, PE-5
A.9.1.4 Protecting against external and environmental threats	CP Family; PE-1, PE-9, PE-10, PE-11, PE-13, PE-15
A.9.1.5 Working in secure areas	AT-2, AT-3 , PL-4, PS-6, PE-2, PE-3, PE-4, PE-6, PE-7, PE-8
A.9.1.6 Public access, delivery and loading areas	PE-3 , PE-7, PE-16
A.9.2 Equipment security	
A.9.2.1 Equipment siting and protection	PE-1, PE-18
A.9.2.2 Supporting utilities	PE-1, PE-9, PE-11, PE-12, PE-14
A.9.2.3 Cabling security	PE-4, PE-9
A.9.2.4 Equipment maintenance	MA Family

ISO/IEC 27001 (Annex A) CONTROLS	NIST SP 800-53 CONTROLS
A.9.2.5 Security of equipment off-premises	MP-5, PE-17
A.9.2.6 Secure disposal or re-use of equipment	MP-6
A.9.2.7 Removal of property	MP-5, PE-16
A.10 Communications and operations management	
A.10.1 Operational procedures and responsibilities	
A.10.1.1 Documented operating procedures	XX-1 controls, CM-9
A.10.1.2 Change management	CM-1, CM-3, CM-4, CM-5, CM-9
A.10.1.3 Segregation of duties	AC-5
A.10.1.4 Separation of development, test and operational facilities	CM-2
A.10.2 Third party service delivery management	
A.10.2.1 Service delivery	SA-9
A.10.2.2 Monitoring and review of third party services	SA-9
A.10.2.3 Managing changes to third party services	RA-3, SA-9
A.10.3 System planning and acceptance	
A.10.3.1 Capacity management	AU-4, AU-5, CP-2, SA-2, SC-5
A.10.3.2 System acceptance	CA-2, CA-6, CM-3, CM-4, CM-9, SA-11
A.10.4 Protection against malicious and mobile code	
A.10.4.1 Controls against malicious code	AC-19, AT-2, SA-8, SC-2, SC-3, SC-7, SC-14, SI-3, SI-7
A.10.4.2 Controls against mobile code	SA-8, SC-2, SC-3, SC-7, SC-14, SC-8, SC-18
A.10.5 Back-up	
A.10.5.1 Information back-up	CP-9
A.10.6 Network security management	
A.10.6.1 Network controls	AC-4, AC-17, AC-20, CA-3, CP-8, PE-5, SC-7, SC-8, SC-9, SC-10, SC-19, SC-20, SC-21, SC-22, SC-23
A.10.6.2 Security of network services	SA-9, SC-8, SC-9
A.10.7 Media handling	
A.10.7.1 Management of removable media	MP Family, PE-16
A.10.7.2 Disposal of media	MP-6
A.10.7.3 Information handling procedures	MP Family, SI-12
A.10.7.4 Security of system documentation	MP-4, SA-5
A.10.8 Exchange of information	
A.10.8.1 Information exchange policies and procedures	AC-1, AC-3, AC-4, AC-17, AC-20, CA-3, PL-4, PS-6, SC-7, SC-16, SI-9
A.10.8.2 Exchange agreements	CA-3, SA-9
A.10.8.3 Physical media in transit	MP-5
A.10.8.4 Electronic messaging	Multiple controls; electronic messaging not addressed separately in SP 800-53
A.10.8.5 Business information systems	CA-1, CA-3
A.10.9 Electronic commerce services	
A.10.9.1 Electronic commerce	AU-10, IA-8, SC-7, SC-8, SC-9, SC-3, SC-14
A.10.9.2 On-line transactions	SC-3, SC-7, SC-8, SC-9, SC-14
A.10.9.3 Publicly available information	SC-14
A.10.10 Monitoring	
A.10.10.1 Audit logging	AU-1, AU-2, AU-3, AU-4, AU-5, AU-8, AU-11, AU-12
A.10.10.2 Monitoring system use	AU-1, AU-6, AU-7, PE-6, PE-8, SC-7, SI-4
A.10.10.3 Protection of log information	AU-9
A.10.10.4 Administrator and operator logs	AU-2, AU-12
A.10.10.5 Fault logging	AU-2, AU-6, AU-12, SI-2
A.10.10.6 Clock synchronization	AU-8
A.11 Access Control	
A.11.1 Business requirement for access control	
A.11.1.1 Access control policy	AC-1, AC-5, AC-6, AC-17, AC-19, CM-5, MP-1, SI-9
A.11.2 User access management	
A.11.2.1 User registration	AC-1, AC-2, AC-21, IA-5, PE-1, PE-2
A.11.2.2 Privilege management	AC-1, AC-2, AC-6, AC-21, PE-1, PE-2, SI-9
A.11.2.3 User password management	IA-5

ISO/IEC 27001 (Annex A) CONTROLS	NIST SP 800-53 CONTROLS
A.11.2.4 Review of user access rights	AC-2, PE-2
A 11.3 User responsibilities	
A.11.3.1 Password use	IA-2, IA-5
A.11.3.2 Unattended user equipment	AC-11, IA-2, PE-3, PE-5, PE-18, SC-10
A.11.3.3 Clear desk and clear screen policy	AC-11
A.11.4 Network access control	
A.11.4.1 Policy on use of network services	AC-1, AC-5, AC-6, AC-17, AC-20
A.11.4.2 User authentication for external connections	AC-17, AC-20, CA-3, IA-2, IA-8
A.11.4.3 Equipment identification in networks	AC-19, IA-3
A.11.4.4 Remote diagnostic and configuration port protection	AC-3, AC-6, AC-17, PE-3, MA-3, MA-4
A.11.4.5 Segregation in networks	AC-4, SA-8, SC-7
A.11.4.6 Network connection control	AC-3, AC-6, AC-17, SC-7
A.11.4.7 Network routing control	AC-4, AC-17
A 11.5 Operating system access control	
A.11.5.1 Secure log-on procedures	AC-7, AC-8, AC-9, AC-10, IA-2, IA-6, IA-8, SC-10
A.11.5.2 User identification and authentication	IA-2, IA-4, IA-5, IA-8
A.11.5.3 Password management system	IA-2, IA-5
A.11.5.4 Use of system utilities	AC-3, AC-6
A.11.5.5 Session time-out	AC-11, SC-10
A.11.5.6 Limitation of connection time	None
A.11.6 Application and information access control	
A.11.6.1 Information access restriction	AC-3, AC-6, AC-14, CM-5
A.11.6.2 Sensitive system isolation	None; SP 800-39
A.11.7 Mobile computing and teleworking	
A.11.7.1 Mobile computing and communications	AC-1, AC-17, AC-19, PL-4, PS-6
A.11.7.2 Teleworking	AC-1, AC-4, AC-17, PE-17, PL-4, PS-6
A.12 Information systems acquisition, development and maintenance	
A.12.1 Security requirements of information systems	
A.12.1.1 Security requirements analysis and specification	SA-1, SA-3, SA-4
A.12.2 Correct processing in applications	
A.12.2.1 Input data validation	SI-10
A.12.2.2 Control of internal processing	SI-7, SI-9, SI-10
A.12.2.3 Message integrity	AU-10, SC-8, SI-7
A.12.2.4 Output data validation	None
A.12.3 Cryptographic controls	
A.12.3.1 Policy on the use of cryptographic controls	Multiple controls address cryptography (e.g., IA-7, SC-8, SC-9, SC-12, SC-13)
A.12.3.2 Key management	SC-12, SC-17
A.12.4 Security of system files	
A.12.4.1 Control of operational software	CM-1, CM-2, CM-3, CM-4, CM-5, CM-9, PL-4, SA-6, SA-7
A.12.4.2 Protection of system test data	Multiple controls; protection of test data not addressed separately in SP 800-53 (e.g., AC-3, AC-4)
A.12.4.3 Access control to program source code	AC-3, AC-6, CM-5, CM-9, MA-5, SA-10
A.12.5 Security in development and support processes	
A.12.5.1 Change control procedures	CM-1, CM-3, CM-9, SA-10
A.12.5.2 Technical review of applications after operating system changes	CM-3, CM-4, CM-9, SI-2
A.12.5.3 Restrictions on changes to software packages	CM-3, CM-4, CM-5, CM-9
A.12.5.4 Information leakage	AC-4, PE-19
A.12.5.5 Outsourced software development	SA-1, SA-4, SA-6, SA-7, SA-8, SA-9, SA-11, SA-12, SA-13
A.12.6 Technical Vulnerability Management	
A.12.6.1 Control of technical vulnerabilities	RA-3, RA-5, SI-2, SI-5
A.13 Information security incident management	
A.13.1 Reporting information security events and weaknesses	
A.13.1.1 Reporting information security events	AU-6, IR-1, IR-6, SI-4, SI-5

ISO/IEC 27001 (Annex A) CONTROLS	NIST SP 800-53 CONTROLS
A.13.1.2 Reporting security weaknesses	PL-4, SI-2, SI-4, SI-5
A.13.2 Management of information security incidents and improvements	
A.13.2.1 Responsibilities and procedures	IR-1
A.13.2.2 Learning from information security incidents	IR-4
A.13.2.3 Collection of evidence	AU-9, IR-4
A.14 Business continuity management	
A.14.1 Information security aspects of business continuity management	
A.14.1.1 Including information security in the business continuity management process	CP-1, CP-2, CP-4
A.14.1.2 Business continuity and risk assessment	CP-2, PM-9, RA Family
A.14.1.3 Developing and implementing continuity plans including information security	CP Family
A.14.1.4 Business continuity planning framework	CP-2, CP-4
A.14.1.5 Testing, maintaining and reassessing business continuity plans	CP-2, CP-4
A.15 Compliance	
A.15.1 Compliance with legal requirements	
A.15.1.1 Identification of applicable legislation	XX-1 controls, IA-7
A.15.1.2 Intellectual property rights (IPR)	SA-6
A.15.1.3 Protection of organizational records	AU-9, AU-11, CP-9, MP-1, MP-4, SA-5, SI-12
A.15.1.4 Data protection and privacy of personal information	PL-5; SI-12
A.15.1.5 Prevention of misuse of information processing facilities	AC-8, AU-6, PL-4, PS-6, PS-8, SA-7
A.15.1.6 Regulation of cryptographic controls	IA-7, SC-13
A.15.2 Compliance with security policies and standards, and technical compliance	
A.15.2.1 Compliance with security policies and standards	XX-1 controls, AC-2, CA-2, CA-7, IA-7, PE-8, SI-12
A.15.2.2 Technical compliance checking	CA-2, CA-7, RA-5
A.15.3 Information systems audit considerations	
A.15.3.1 Information systems audit controls	AU-1, AU-2, PL-6
A.15.3.2 Protection of information systems audit tools	AU-9

APPENDIX I

INDUSTRIAL CONTROL SYSTEMS

SECURITY CONTROLS, ENHANCEMENTS, AND SUPPLEMENTAL GUIDANCE

Industrial control systems (ICS)[55] are information systems that differ significantly from traditional administrative, mission support, and scientific data processing information systems. ICS typically have many unique characteristics—including a need for real-time response and extremely high availability, predictability, and reliability. These types of specialized systems are pervasive throughout the critical infrastructure, often being required to meet several and often conflicting safety, operational, performance, reliability, and security requirements such as: (i) minimizing risk to the health and safety of the public; (ii) preventing serious damage to the environment; (iii) preventing serious production stoppages or slowdowns that result in negative impact to the Nation's economy and ability to carry out critical functions; (iv) protecting the critical infrastructure from cyber attacks and common human error; and (v) safeguarding against the compromise of proprietary information.[56]

Until recently, ICS had little resemblance to traditional information systems in that they were isolated systems running proprietary software and control protocols. However, as these systems have been increasingly integrated more closely into mainstream organizational information systems to promote connectivity, efficiency, and remote access capabilities, they have started to resemble the more traditional information systems. Increasingly, ICS use the same commercially available hardware and software components as are used in the organization's traditional information systems. While the change in industrial control system architecture supports new information system capabilities, it also provides significantly less isolation from the outside world for these systems, introducing many of the same vulnerabilities that exist in current networked information systems. The result is an even greater need to secure ICS.

FIPS 200, in combination with NIST Special Publication 800-53, requires that federal agencies (and organizations subordinate to those agencies) implement minimum security controls for their organizational information systems based on the FIPS 199 security categorization of those systems. This includes implementing the baseline security controls described in NIST Special Publication 800-53 in ICS that are operated by or on behalf of federal agencies. Section 3.3, *Tailoring the Initial Baseline*, allows organizations[57] to modify or adjust recommended security control baselines when certain conditions exist that require that flexibility. NIST recommends that ICS owners take advantage of the ability to tailor the initial baselines applying the ICS-specific guidance in this appendix. This appendix also contains additions to the initial security control baselines that have been determined to be generally required for ICS.

[55] An ICS is an information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and programmable logic controllers (PLC). ICS are typically found in the electric, water, oil and gas, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (automotive, aerospace, and durable goods) industries as well as in air and rail transportation control systems.

[56] See Executive Order 13231 on Critical Infrastructure Protection, October 16, 2001.

[57] NIST Special Publication 800-53 employs the term *organization* to refer to the owner or operator of an information system. In this Appendix, organization may refer to the owner or operator of an ICS.

NIST has worked cooperatively with ICS communities in the public and private sectors to develop specific guidance on the application of the security controls in Special Publication 800-53 to ICS. That guidance, contained in this Appendix, includes ICS-specific:

- Tailoring guidance;
- Security control enhancements;
- Supplements to the security control baselines; and
- Supplemental guidance.

ICS Tailoring Guidance

Tailoring guidance for ICS can include scoping guidance and the application of compensating security controls. Due to the unique characteristics of ICS, these systems may require a greater use of compensating security controls than is the case for general purpose information systems.

> **In situations where the ICS cannot support, or the organization determines it is not advisable to implement particular security controls or control enhancements in an ICS (e.g., performance, safety, or reliability are adversely impacted), the organization provides a complete and convincing rationale for how the selected compensating controls provide an equivalent security capability or level of protection for the ICS and why the related baseline security controls could not be employed.**
>
> **If the ICS cannot support the use of automated mechanisms, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance in Section 3.3.**
>
> **Compensating controls are not exceptions or waivers to the baseline controls; rather, they are alternative safeguards and countermeasures employed within the ICS that accomplish the intent of the original security controls that could not be effectively employed. Organizational decisions on the use of compensating controls are documented in the security plan for the ICS.**

The security controls and control enhancements listed in Table I-1 are likely candidates for tailoring (i.e., requiring the application of scoping guidance and/or compensating controls) with regard to ICS. Note that the parenthetical numbers following the control identification refer to control enhancements.

TABLE I-1: SECURITY CONTROL CANDIDATES FOR TAILORING

CONTROL NUMBER	CONTROL NAME	TAILORING OPTIONS	
		SCOPING GUIDANCE	COMPENSATING CONTROLS
AC-2	Account Management	NO	YES
AC-2(1)	Account Management	YES	YES
AC-5	Separation of Duties	NO	YES
AC-6	Least Privilege	NO	YES
AC-7	Unsuccessful Login Attempts	NO	YES
AC-8	System Use Notification	NO	YES
AC-10	Concurrent Session Control	NO	YES
AC-11	Session Lock	NO	YES
AC-16	Automated Labeling	YES	YES
AC-17(1)	Remote Access	YES	YES
AC-17(2)	Remote Access	NO	YES
AU-2	Auditable Events	NO	YES
AU-6	Audit Review, Analysis, and Reporting	NO	YES
AU-7	Audit Reduction and Report Generation	NO	YES
CA-2	Security Assessments	NO	YES
CM-3(1)	Configuration Change Control	YES	YES
CM-3(ICS-1)	Configuration Change Control	NO	YES
CM-5(1)	Access Restrictions for Change	YES	YES
CM-6(1)	Configuration Settings	YES	YES
CP-4	Contingency Plan Testing and Exercises	NO	YES
CP-7	Alternate Processing Site	NO	YES
IA-2	User Identification and Authentication	NO	YES
IA-3	Device Identification and Authentication	NO	YES
MA-3 (4)	Maintenance Tools	YES	YES
MA-4 (3)	Remote Maintenance	YES	YES
MP-3	Media Marking	YES	YES
PE-6 (2)	Monitoring Physical Access	YES	YES
RA-5	Vulnerability Scanning	NO	YES
SC-3	Security Function Isolation	NO	YES
SC-10	Network Disconnect	NO	YES
SI-2 (1)	Flaw Remediation	YES	YES
SI-2 (2)	Flaw Remediation	YES	YES
SI-3 (1)	Malicious Code Protection	YES	YES
SI-3 (2)	Malicious Code Protection	YES	YES
SI-6 (2)	Security Functionality Verification	YES	YES
SI-8 (1)	Spam Protection	YES	YES
SI-8 (2)	Spam Protection	YES	YES

ICS Supplements to the Security Control Baselines

The following table lists the recommended ICS supplements (highlighted in **bold** text) to the security control baselines in Appendix D.

TABLE I-2: ICS SUPPLEMENTS TO SECURITY CONTROL BASELINES

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
Access Control				
AC-3	Access Enforcement	AC-3	AC-3 (1) **(2)**	AC-3 (1) **(2)**
Physical and Environmental Protection				
PE-9	Power Equipment and Power Cabling	Not Selected	PE-9 **(1)**	PE-9 **(1)**
PE-11	Emergency Power	**PE-11**	PE-11 **(1)**	PE-11 (1) **(2)**
System and Information Integrity				
SI-13	Predictable Failure Prevention	Not Selected	Not-selected	**SI-13**

In addition to the enhancements added for ICS in the table above, the security control supplement process described in Section 3.4 is still applicable to ICS. Organizations are required to conduct a risk assessment taking into account the tailoring and supplementing performed in arriving at the agreed upon set of security controls for the ICS and the risk to the organization's operations and assets, individuals, other organizations, and the Nation being incurred by operation of the ICS with the intended controls. The organization decides whether that risk is acceptable, and if not, supplements the control set with additional controls until an acceptable level of risk is obtained.

ICS Supplemental Guidance

ICS Supplemental Guidance provides organizations with additional information on the application of the security controls and control enhancements in Appendix F to ICS and the environments in which these specialized systems operate. The Supplemental Guidance also provides information as to why a particular security control or control enhancement may not be applicable in some ICS environments and may be a candidate for tailoring (i.e., the application of scoping guidance and/or compensating controls). ICS Supplemental Guidance does not replace the original Supplemental Guidance in Appendix F.

ACCESS CONTROL

AC-2 ACCOUNT MANAGEMENT

ICS Supplemental Guidance: In situations where physical access to the ICS (e.g., workstations, hardware components, or field devices) predefines account privileges or where the ICS (e.g., certain remote terminal units, meters, or relays) cannot support account management, the organization employs appropriate compensating controls (e.g., providing increased physical security, personnel security, intrusion detection, and auditing measures) in accordance with the general tailoring guidance.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS (e.g., field devices) cannot support the use of automated mechanisms for the management of information system accounts, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-3 ACCESS ENFORCEMENT

ICS Supplemental Guidance: The organization ensures that access enforcement mechanisms do not adversely impact the operational performance of the ICS. NIST Special Publication 800-82 provides guidance on ICS access enforcement.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: Within ICS, it is commonly the case that having access to specific devices (e.g., workstations, remote terminal units, field devices) is the equivalent to having privileged access; thereby restricting access to these devices is also restricting access to privileged functions and security-relevant information.

AC-5 SEPARATION OF DUTIES

ICS Supplemental Guidance: In situations where the ICS cannot support the differentiation of roles or a single individual performs all roles within the ICS, the organization employs appropriate compensating controls (e.g., providing increased personnel security and auditing measures) in accordance with the general tailoring guidance.

AC-6 LEAST PRIVILEGE

ICS Supplemental Guidance: In situations where the ICS cannot support differentiation of privileges or a single individual performs all roles within the ICS, the organization employs appropriate compensating controls (e.g., providing increased personnel security and auditing measures) in accordance with the general tailoring guidance.

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

ICS Supplemental Guidance: In situations where the ICS cannot support account/node locking or delayed login attempts, or the ICS cannot perform account/node locking or delayed logins due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., logging or recording all unsuccessful login attempts and alerting ICS security personnel though alarms or other means when the number of organization-defined consecutive invalid access attempts is exceeded) in accordance with the general tailoring guidance.

AC-8 SYSTEM USE NOTIFICATION

ICS Supplemental Guidance: In situations where the ICS cannot support system use notification, the organization employs appropriate compensating controls (e.g., posting physical notices in ICS facilities) in accordance with the general tailoring guidance.

AC-10 CONCURRENT SESSION CONTROL

ICS Supplemental Guidance: In situations where the ICS cannot support concurrent session control, the organization employs appropriate compensating controls (e.g., providing increased auditing measures) in accordance with the general tailoring guidance.

AC-11 SESSION LOCK

ICS Supplemental Guidance: The ICS employs session lock to prevent access to specified workstations/nodes. The ICS activates session lock mechanisms automatically after an organization-defined time period for designated workstations/nodes on the ICS. In some cases, session lock for ICS operator workstations/nodes is not advised (e.g., when immediate operator responses are required in emergency situations). Session lock is not a substitute for logging out of the ICS. In situations where the ICS cannot support session lock, the organization employs appropriate compensating controls (e.g., providing increased physical security, personnel security, and auditing measures) in accordance with the general tailoring guidance. NIST Special Publication 800-82 provides guidance on the use of session lock within an ICS environment.

AC-16 AUTOMATED LABELING

ICS Supplemental Guidance: In situations where the ICS cannot support automated labeling of ICS information in process, in storage, or in transit, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-17 REMOTE ACCESS

ICS Supplemental Guidance: NIST Special Publication 800-82 defines and provides guidance on ICS remote access.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms for monitoring and control of remote access methods, the organization employs nonautomated mechanisms or procedures as compensating controls (e.g., following manual authentication [see IA-2 in this appendix], dial-in remote access may be enabled for a specified period of time or a call may be placed from the ICS site to the authenticated remote entity) in accordance with the general tailoring guidance.

Control Enhancement: (2)

ICS Enhancement Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. In situations where the ICS cannot support the use of cryptographic mechanisms to protect the confidentiality and integrity of remote sessions, or the components cannot use cryptographic mechanisms due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., providing increased auditing measures for remote sessions or limiting remote access privileges to key personnel) in accordance with the general tailoring guidance.

AWARENESS AND TRAINING

AT-2 SECURITY AWARENESS

ICS Supplemental Guidance: Security awareness training includes initial and periodic review of ICS-specific policies, standard operating procedures, security trends, and vulnerabilities. The ICS security awareness program is consistent with the requirements of the security awareness and training policy established by the organization.

AT-3 SECURITY TRAINING

ICS Supplemental Guidance: Security training includes initial and periodic review of ICS-specific policies, standard operating procedures, security trends, and vulnerabilities. The ICS security training program is consistent with the requirements of the security awareness and training policy established by the organization.

AUDITING AND ACCOUNTABILITY

AU-2 AUDITABLE EVENTS

ICS Supplemental Guidance: Most ICS auditing occurs at the application level. In situations where the ICS cannot support the use of automated mechanisms to generate audit records, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

ICS Supplemental Guidance: In general, audit record processing is not performed on the ICS, but on a separate information system. In situations where the ICS cannot support auditing including response to audit failures, the organization employs compensating controls (e.g., providing an auditing capability on a separate information system) in accordance with the general tailoring guidance.

AU-7 AUDIT REDUCTION AND REPORT GENERATION

ICS Supplemental Guidance: In general, audit reduction and report generation is not performed on the ICS, but on a separate information system. In situations where the ICS cannot support auditing including audit reduction and report generation, the organization employs compensating controls (e.g., providing an auditing capability on a separate information system) in accordance with the general tailoring guidance.

SECURITY ASSESSMENT AND AUTHORIZATION

CA-2 SECURITY ASSESSMENTS

ICS Supplemental Guidance: Assessments are performed and documented by qualified assessors (e.g., experienced in assessing ICS) authorized by the organization. The organization ensures that assessments do not interfere with ICS functions. The individual/group conducting the assessment fully understands the organizational information security policies and procedures, the ICS security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. A production ICS may need to be taken off-line, or replicated to the extent feasible, before an assessment can be conducted. If an ICS must be taken off-line to conduct an assessment, the assessment is scheduled to occur during planned ICS outages whenever possible. In situations where the organization cannot, for operational reasons, conduct a live assessment of a production ICS, the organization employs compensating controls (e.g., providing a replicated system to conduct the assessment) in accordance with the general tailoring guidance.

CONFIGURATION MANAGEMENT

CM-3 CONFIGURATION CHANGE CONTROL

ICS Supplemental Guidance: NIST Special Publication 800-82 provides guidance on configuration change control for ICS.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to implement configuration change control, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

CM-4 SECURITY IMPACT ANALYSIS

ICS Supplemental Guidance: The organization considers ICS safety and security interdependencies.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to enforce access restrictions and support auditing of enforcement actions, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

CM-6 CONFIGURATION SETTINGS

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to centrally manage, apply, and verify configuration settings, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

CONTINGENCY PLANNING

CP-2 CONTINGENCY PLAN

ICS Supplemental Guidance: The organization defines contingency plans for categories of disruptions or failures. In the event of a loss of processing within the ICS or communication with operational facilities, the ICS executes predetermined procedures (e.g., alert the operator of the failure and then do nothing, alert the operator and then safely shut down the industrial process, alert the operator and then maintain the last operational setting prior to failure). These examples are not exhaustive. NIST Special Publication 800-82 provides guidance on ICS failure modes.

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

ICS Supplemental Guidance: In situations where the organization cannot test or exercise the contingency plan on production ICS due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., using scheduled and unscheduled system maintenance activities including responding to ICS component and system failures, as an opportunity to test or exercise the contingency plan) in accordance with the general tailoring guidance.

CP-7 ALTERNATE PROCESSING SITE

ICS Supplemental Guidance: In situations where the organization cannot provide an alternate processing site, the organization employs appropriate compensating controls in accordance with the general tailoring guidance.

IDENTIFICATION AND AUTHENTICATION

IA-2 USER IDENTIFICATION AND AUTHENTICATION

ICS Supplemental Guidance: Where users function as a single group (e.g., control room operators), user identification and authentication may be role-based, group-based, or device-based. For certain ICS, the capability for immediate operator interaction is critical. Local emergency actions for ICS are not hampered by identification or authentication requirements. Access to these systems may be restricted by appropriate physical security controls. In situations where the ICS cannot support user identification and authentication, or the organization determines it is not advisable to perform user identification and authentication due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., providing increased physical security, personnel security, and auditing measures) in accordance with the general tailoring guidance. For example, manual voice authentication of remote personnel and local, manual actions may be required in order to establish a remote access [see AC-17 in this appendix]. NIST Special Publication 800-82 provides guidance on ICS user identification and authentication. Local user access to ICS components is enabled only when necessary, approved, and authenticated.

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

ICS Supplemental Guidance: In situations where the ICS cannot support device identification and authentication (e.g., serial devices), the organization employs compensating controls in accordance with the general tailoring guidance.

IA-4 IDENTIFIER MANAGEMENT

ICS Supplemental Guidance: Where users function as a single group (e.g., control room operators), user identification may be role-based, group-based, or device-based. NIST Special Publication 800-82 provides guidance on ICS identifier management.

IA-5 AUTHENTICATOR MANAGEMENT

ICS Supplemental Guidance: NIST Special Publication 800-82 provides guidance on ICS authenticator management.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

ICS Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

INCIDENT RESPONSE

IR-6 INCIDENT REPORTING

ICS Supplemental Guidance: Each organization establishes reporting criteria, to include sharing information through appropriate channels. The United States Computer Emergency Readiness Team (US-CERT) maintains the ICS Security Center at http://www.uscert.gov/control_systems. NIST Special Publication 800-82 provides guidance on ICS incident reporting.

MAINTENANCE

MA-3 MAINTENANCE TOOLS

Control Enhancement: (4)

ICS Enhancement Supplemental Guidance: In situations where the organization cannot employ automated mechanisms to restrict the use of maintenance tools for the ICS, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

MA-4 REMOTE MAINTENANCE

Control Enhancement: (3)

ICS Enhancement Supplemental Guidance: In crisis or emergency situations, the organization may need immediate access to remote maintenance and diagnostic services in order to restore essential ICS operations or services. In situations where the organization may not have access to the required level of remote maintenance or diagnostic service provider security capability, the organization employs appropriate compensating controls (e.g., limiting the extent of the maintenance and diagnostic services to the minimum essential activities, and/or carefully monitoring and auditing the remote maintenance and diagnostic activities) in accordance with the general tailoring guidance.

MEDIA PROTECTION

MP-3 MEDIA MARKING

ICS Supplemental Guidance: In situations where the ICS cannot support automated marking of output, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

PHYSICAL AND ENVIRONMENTAL PROTECTION

PE-3 PHYSICAL ACCESS CONTROL

ICS Supplemental Guidance: The organization considers ICS safety and security interdependencies. The organization considers access requirements in emergency situations. During an emergency-related event, the organization may restrict access to ICS facilities and assets to authorized individuals only. ICS are often constructed of devices that either do not have or cannot use comprehensive access control capabilities due to time-restrictive safety constraints. Physical access controls and defense-in-depth measures are used by the organization when necessary and possible to supplement ICS security when electronic mechanisms are unable to fulfill the security requirements of the organization's security plan. NIST Special Publication 800-82 provides guidance on ICS physical access control.

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

ICS Supplemental Guidance: This control applies to ICS communications infrastructure (e.g., satellite ground stations, microwave towers) within organizational facilities.

PE-6 MONITORING PHYSICAL ACCESS

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: In situations where the organization cannot employ automated mechanisms to recognize potential intrusions to the ICS and to initiate appropriate response actions, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

PLANNING

PL-2 SYSTEM SECURITY PLAN

ICS Supplemental Guidance: NIST Special Publication 800-82 provides guidance on developing ICS security plans.

RISK ASSESSMENT

RA-2 SECURITY CATEGORIZATION

ICS Supplemental Guidance: NIST Special Publication 800-82 provides guidance on ICS security categorizations.

RA-3 RISK ASSESSMENT

ICS Supplemental Guidance: NIST Special Publication 800-82 provides guidance on ICS risk assessments.

RA-5 VULNERABILITY SCANNING

ICS Supplemental Guidance: Vulnerability scanning tools are used with care on ICS networks to ensure that ICS functions are not adversely impacted by the scanning process. Production ICS may need to be taken off-line, or replicated to the extent feasible, before scanning can be conducted. If ICS are taken off-line for scanning, scans are scheduled to occur during planned ICS outages whenever possible. If vulnerability scanning tools are used on non-ICS networks, extra care is taken to ensure that they do not scan the ICS network. In situations where the organization cannot, for operational reasons, conduct vulnerability scanning on a production ICS, the organization employs compensating controls (e.g., providing a replicated system to conduct scanning) in accordance with the general tailoring guidance. NIST Special Publication 800-82 provides guidance on ICS vulnerability scanning.

SYSTEM AND SERVICES ACQUISITION

SA-4 ACQUISITIONS

ICS Supplemental Guidance: The SCADA and Control Systems Procurement Project provides example cyber security procurement language for ICS. See http://www.msisac.org/scada.

SA-8 SECURITY ENGINEERING PRINCIPLES

ICS Supplemental Guidance: NIST Special Publication 800-82 provides guidance on ICS defense-in-depth protection strategy.

SYSTEM AND COMMUNICATIONS PROTECTION

SC-3 SECURITY FUNCTION ISOLATION

ICS Supplemental Guidance: In situations where the ICS cannot support security function isolation, the organization employs compensating controls (e.g., providing increased auditing measures, limiting network connectivity) in accordance with the general tailoring guidance.

SC-7 BOUNDARY PROTECTION

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: Generally, public access to ICS information is not permitted.

SC-8 TRANSMISSION INTEGRITY

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

SC-9 TRANSMISSION CONFIDENTIALITY

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

SC-10 NETWORK DISCONNECT

ICS Supplemental Guidance: In situations where the ICS cannot terminate a network connection at the end of a session or after an organization-defined time period of inactivity, or the ICS cannot terminate a network connection due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., providing increased auditing measures or limiting remote access privileges to key personnel) in accordance with the general tailoring guidance.

SC-13 USE OF CRYPTOGRAPHY

ICS Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

SC-14 PUBLIC ACCESS PROTECTIONS

ICS Supplemental Guidance: Generally, public access to ICS is not permitted.

SC-15 COLLABORATIVE COMPUTING DEVICES

ICS Supplemental Guidance: Generally, collaborative computing mechanisms are not permitted on ICS.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

ICS Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. The use of Public Key Infrastructure technology in ICS is intended to support internal nonpublic use.

SC-19 VOICE OVER INTERNET PROTOCOL

ICS Supplemental Guidance: Generally, VoIP technologies are not permitted on ICS. The use of VoIP technologies is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SYSTEM AND INFORMATION INTEGRITY

SI-2 FLAW REMEDIATION

ICS Supplemental Guidance: NIST SP 800-82 provides guidance on flaw remediation in ICS.

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: In situations where the organization cannot centrally manage flaw remediation and automatic updates, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to conduct and report on the status of flaw remediation, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

SI-3 MALICIOUS CODE PROTECTION

ICS Supplemental Guidance: The use of malicious code protection is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS. NIST Special Publication 800-82 provides guidance on implementing ICS malicious code protection.

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: In situations where the organization cannot centrally manage malicious code protection mechanisms, the organization employs appropriate compensating controls in accordance with the general tailoring guidance.

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to update malicious code protection mechanisms, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

SI-4 INFORMATION SYSTEM MONITORING

ICS Supplemental Guidance: The organization ensures that the use of monitoring tools and techniques does not adversely impact the operational performance of the ICS.

SI-6 SECURITY FUNCTIONALITY VERIFICATION

ICS Supplemental Guidance: Generally, it is not recommended to shut down and restart the ICS upon the identification of an anomaly.

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms for the management of distributed security testing, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

SI-7 SOFTWARE AND INFORMATION INTEGRITY

ICS Supplemental Guidance: The organization ensures that the use of integrity verification applications does not adversely impact the operational performance of the ICS.

SI-8 SPAM PROTECTION

ICS Supplemental Guidance: The organization removes unused and unnecessary functions and services (e.g., electronic mail, Internet access). Due to differing operational characteristics between ICS and general purpose information systems, ICS do not generally employ spam protection mechanisms. Unusual traffic flow (e.g., during crisis situations), may be misinterpreted and detected as spam, which can cause issues with the ICS and possible system failure.

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: In situations where the organization cannot centrally manage spam protection mechanisms, the organization employs appropriate compensating controls in accordance with the general tailoring guidance.

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to update spam protection mechanisms, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.