FIPS PUB 200

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Minimum Security Requirements for Federal Information and Information Systems

---

INITIAL PUBLIC DRAFT

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

July 2005

U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary

TECHNOLOGY ADMINISTRATION
Michelle O'Neill, Acting Under Secretary of Commerce for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Hratch G. Semerjian, Acting Director

FOREWORD

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA) of 2002. Comments concerning FIPS publications are welcomed and should be addressed to the Director, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900.

-- DR. SHASHI PHOHA, DIRECTOR
INFORMATION TECHNOLOGY LABORATORY

AUTHORITY

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347).

NOTES TO REVIEWERS

FIPS Publication 200 is one of a series of security standards and guidelines being developed by NIST in response to the FISMA legislation. FIPS Publication 200 provides: (i) a specification for minimum security requirements for federal information and information systems; (ii) a standardized approach to security control selection using the security categorization standard, FIPS Publication 199; and (iii) links to NIST Special Publication 800-53, containing the security controls needed for compliance with these minimum security requirements. The proposed security standard is an integral part of the risk management framework developed by NIST as part of the FISMA Implementation Project that effectively integrates all of the security standards and guidelines supporting the implementation of the legislation.

NIST invites federal agencies and the public to review and comment upon this proposed security standard. We are interested in your feedback on: (i) the general approach of FIPS Publication 200 in providing high-level minimum security requirements and the linkage of the standard to NIST Special Publication 800-53; (ii) the content of the individual minimum security requirements; (iii) the standardized approach for selecting security controls from NIST Special Publication 800-53 based on the security categorization of information systems using FIPS Publication 199 and NIST Special Publication 800-60; and (iv) the cost and potential impact (including security benefits) on organizations and individuals in employing the minimum security requirements and the associated security controls needed to satisfy those requirements.

Comments will be accepted through September 13, 2005. NIST plans to thoroughly review and assess all comments received during the public vetting process, revise the proposed standard as needed, and publish the final standard and general responses to the public comments in the Federal Register upon approval of the Secretary of Commerce. Written comments may be sent to: Chief, Computer Security Division, Information Technology Laboratory, Attention: Comments on Draft FIPS Publication 200, 100 Bureau Drive (Stop 8930), National Institute of Standards and Technology, Gaithersburg, MD 20899-8930. Comments may also be sent via electronic mail to: draftfips200@nist.gov. A copy of draft FIPS Publication 200 is available from the NIST Computer Security Resource Center website at: http://csrc.nist.gov/publications/fips/index.html.

The FISMA Implementation Project main web site at http://csrc.nist.gov/sec-cert contains valuable information on all of the FISMA-related security standards and guidelines and how the publications can be used to manage enterprise risk and build a comprehensive information security program.

We have attempted to provide a security standard that establishes a level of security due diligence for federal agencies in protecting their information and information systems. FIPS Publication 200 uses a risk-based approach that facilitates cost-effective information security. Your feedback to us, as always, is critical in the security standards and guidelines development process to ensure that the work products produced by NIST are meeting the security needs of the federal government and those in the private sector who voluntarily use our products.

-- RON ROSS
PROJECT LEADER, FISMA IMPLEMENTATION PROJECT

Federal Information Processing Standards 200

[*Insert date of Secretarial approval*]

Announcing the Standard for
Minimum Security Requirements for
Federal Information and Information Systems

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to the Federal Information Security Management Act (FISMA) of 2002.

1. Name of Standard.

FIPS Publication 200: Minimum Security Requirements for Federal Information and Information Systems.

2. Category of Standard.

Information Security.

3. Explanation.

The E-Government Act (P.L. 107-347) passed by the one hundred and seventh Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the Electronic Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for each federal agency to develop, document, and implement an enterprise-wide program to provide information security for the information and information systems that support the operations and assets of the agency including those provided or managed by another agency, contractor, or other source. FISMA directed the promulgation of federal standards for: (i) the security categorization of federal information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; and (ii) minimum security requirements for information and information systems in each such category. This standard addresses the specification of minimum security requirements for federal information systems.

4. Approving Authority.

Secretary of Commerce.

5. Maintenance Agency.

Department of Commerce, NIST, Information Technology Laboratory (ITL).

6. Applicability.

This standard is applicable to: (i) all information within the federal government other than that 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; and (ii) all federal information systems other than those information systems designated as national security systems as defined in 44 United States Code Section 3542(b)(2). The standard has been broadly developed from a technical perspective to complement similar standards for national security systems. In addition to the agencies of the federal government, state, local, and tribal governments, and private sector organizations that compose the critical infrastructure of the United States are encouraged to consider the use of this standard, as appropriate.

7. Specifications.

Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems.*

8. Implementations.

This standard specifies minimum security requirements for federal information and information systems in seventeen security-related areas. Federal agencies must meet the minimum security requirements defined herein through the use of the security controls in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, as amended.

9. Effective Date.

This standard is effective immediately. Federal agencies must be in compliance with this standard not later than one year from its effective date.

10. Qualifications.

The application of the security controls defined in NIST Special Publication 800-53 required by this standard represent the current state-of-the-practice safeguards and countermeasures for information systems. The security controls will be reviewed by NIST at least annually and, if necessary, revised and extended to reflect: (i) the experience gained from using the controls; (ii) the changing security requirements within federal agencies; and (iii) the new security technologies that may be available. The minimum security controls defined in the low, moderate, and high security control baselines are also expected to change over time as well, as the level of security and due diligence for mitigating risks within federal agencies increases. The proposed additions, deletions, or modifications to the catalog of security controls and the proposed changes to the security control baselines in NIST Special Publication 800-53 will go through a rigorous, public review process to obtain government and private sector feedback and to build consensus for the changes. Federal agencies will have up to one year from the date of final publication to fully comply with the changes but are encouraged to initiate compliance activities immediately.

11. Waivers.

No provision is provided under FISMA for waivers to the Federal Information Processing Standards made mandatory by the Secretary of Commerce.

12. Where to Obtain Copies.

This publication is available from the NIST Computer Security Division web site by accessing http://csrc.nist.gov/publications.

TABLE OF CONTENTS

1 PURPOSE

The E-Government Act of 2002 (Public Law 107-347), passed by the one hundred and seventh Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA), tasked NIST with the responsibility of developing security standards and guidelines for the federal government including the development of:

- Standards for categorizing information and information systems[1] collected or maintained by or on behalf of each federal agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;
- Guidelines recommending the types of information and information systems to be included in each category; and
- Minimum information security requirements for information and information systems in each such category.

FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, approved by the Secretary of Commerce in February 2004, created the first of two mandatory security standards required by the FISMA legislation. FIPS Publication 200, the second of the mandatory security standards, specifies minimum security requirements for information and information systems supporting the executive agencies of the federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements. This standard will promote the development, implementation, and operation of more secure information systems within the federal government by establishing minimum levels of due diligence for information security and facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems that meet minimum security requirements.

2 INFORMATION SYSTEM IMPACT LEVELS

FIPS Publication 199 requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The potential impact values assigned to the respective security objectives are the highest values (i.e., high water mark[2]) from among the security categories that have been determined for each type of information resident on those information systems.[3] 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.

[1] An *information system* is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information resources include information and related resources, such as personnel, equipment, funds, and information technology.

[2] 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.

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

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 must be used to determine the overall impact level of the information system. Thus, a *low-impact system* is 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. The determination of information system impact levels must be accomplished prior to the consideration of minimum security requirements and the selection of appropriate security controls for those information systems.

3 MINIMUM SECURITY REQUIREMENTS

The minimum security requirements cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems. The specific security-related areas include: (i) access control; (ii) awareness and training; (iii) audit and accountability; (iv) certification, accreditation, and security assessments; (v) configuration management; (vi) contingency planning; (vii) identification and authentication; (viii) incident response; (ix) maintenance; (x) media protection; (xi) physical and environmental protection; (xii) planning; (xiii) personnel security; (xiv) risk assessment; (xv) systems and services acquisition; (xvi) system and communications protection; and (xvii) system and information integrity. The seventeen areas represent a broad-based, balanced information security program that addresses the management, operational, and technical aspects of protecting federal information and information systems. Organizations[4] must meet the minimum security requirements in this standard by applying security controls selected in accordance with NIST Special Publication 800-53 and the designated impact levels of the respective organizational information systems as determined during the security categorization process.

Policies and procedures play an important role in the effective implementation of enterprise-wide information security programs within the federal government and the success of the resulting security measures employed to protect federal information and information systems. Thus, organizations must develop and promulgate formal, documented policies and procedures governing the minimum security requirements set forth in this standard and must ensure their effective implementation.

Specifications for Minimum Security Requirements

Access Control (AC): Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and Training (AT): Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Audit and Accountability (AU): Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

[4] The term *organization* is used throughout this standard to mean a federal agency or, as appropriate, any of its operational elements.

Certification, Accreditation, and Security Assessments (CA): Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Configuration Management (CM): Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems; (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems; and (iii) monitor and control changes to the baseline configurations and to the constituent components of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Contingency Planning (CP): Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and Authentication (IA): Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Incident Response (IR): Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance (MA): Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Media Protection (MP): Organizations must: (i) protect information contained in organizational information systems in printed form or on digital media; (ii) limit access to information in printed form or on digital media removed from organizational information systems to authorized users; and (iii) sanitize or destroy digital media before disposal or release for reuse.

Physical and Environmental Protection (PE): Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Planning (PL): Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Personnel Security (PS): Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Risk Assessment (RA): Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

System and Services Acquisition (SA): Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect outsourced organizational information, applications, and/or services.

System and Communications Protection (SC): Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and Information Integrity (SI): Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

4 SECURITY CONTROL SELECTION

Organizations must meet the minimum security requirements in this standard by selecting the appropriate security controls and assurance requirements as described in NIST Special Publication 800-53. The process of selecting the appropriate security controls and assurance requirements for organizational information systems to achieve *adequate security*[5] is a multifaceted, risk-based activity involving management and operational personnel within the organization. Security categorization of federal information and information systems, as required by FIPS Publication 199, is the first step in the risk management process.[6] Subsequent to the security categorization process, organizations must select an appropriate set of security controls for their information systems that satisfy the minimum security requirements set forth in this standard. The selected set of security controls must be one of three security control baselines from NIST Special Publication 800-53 that are associated with the designated impact levels of the organizational information systems as determined during the security categorization process.

- For *low-impact* information systems, organizations must, as a minimum, employ the security controls from the low baseline of security controls defined in NIST Special Publication 800-53 and must ensure that the minimum assurance requirements associated with the low baseline are satisfied.
- For *moderate-impact* information systems, organizations must, as a minimum, employ the security controls from the moderate baseline of security controls defined in NIST Special Publication 800-53 and must ensure that the minimum assurance requirements associated with the moderate baseline are satisfied.
- For *high-impact* information systems, organizations must, as a minimum, employ the security controls from the high baseline of security controls defined in NIST Special Publication 800-53 and must ensure that the minimum assurance requirements associated with the high baseline are satisfied.

[5] The Office of Management and Budget (OMB) Circular A-130, Appendix III, defines *adequate security* as security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

[6] Security categorization must be accomplished as an enterprise-wide activity with the involvement of senior-level organizational officials including, but not limited to, chief information officers, senior agency information security officers, authorizing officials (a.k.a. accreditation authorities), information system owners, and information owners. NIST Special Publication 800-60 provides implementation guidance for FIPS Publication 199.

Organizations must employ all security controls in the respective security control baselines unless specific exceptions are allowed based on the application of scoping guidance or the specification of compensating security controls, the provisions of which are described in the next section.

5 TAILORING THE SECURITY CONTROL BASELINE

Organizations have the flexibility to tailor the security control baselines in accordance with the terms and conditions set forth in this standard. Tailoring activities include: (i) the application of appropriate scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls, where allowed. To ensure a cost-effective, risk-based approach to achieving adequate security across the organization, security control baseline tailoring activities must be coordinated with and approved by appropriate organizational officials (e.g., chief information officers, senior agency information security officers, authorizing officials, or authorizing officials designated representatives). The resulting set of security controls must be documented in the security plan for the information system.

Scoping Guidance

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

Technology-related considerations—

- Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) will only be applicable if those technologies are employed or are required to be employed within the information system.
- Security controls will only be applicable to those components of the information system that typically provide the security capability addressed by the minimum security requirements.[7]
- Security controls that can be either explicitly or implicitly supported by automated mechanisms, will not require the development of such mechanisms if the mechanisms do not already exist or are not readily available in commercial or government off-the-shelf products. In situations where automated mechanisms are not readily available or technically feasible, compensating security controls, implemented through non automated mechanisms or procedures will be used to satisfy minimum security requirements. (See terms and conditions for applying compensating controls.)

Common security control-related considerations—

- Security controls designated by the organization as common controls will in most cases, be managed by an organizational entity other than the information system owner. Every control in a security control baseline must be addressed either by the organization through common security controls or by the information system owner. Decisions on common control designations must not, however, affect the organization's responsibility in providing the necessary security controls required to meet the minimum security requirements for the information system.

[7] For example, auditing controls would typically be applied to the components of an information system that provide or are required to provide auditing capability (mainframes, servers, etc.) and would not necessarily be applied to every user-level workstation within the organization. Access control mechanisms would not typically be applied to such devices as personal digital assistants, facsimile machines, printers, pagers, cellular telephones, or other components of an information system that provide limited functionality. Organizations should, however, carefully assess the inventory of components that make up their information systems to determine which security controls are applicable to the various components. As technology advances, increased functionality may be present in such devices, which may require the application of security controls in accordance with an organizational assessment of risk.

Public access information systems-related considerations—

- Security controls associated with public access information systems must be carefully considered and applied with discretion since some of the security controls from the specified security control baselines (e.g., personnel security controls, identification and authentication controls) may not be applicable to users accessing information systems through public interfaces.[8]

Infrastructure-related considerations—

- Security controls that refer to organizational facilities (e.g., physical access controls such as locks and guards, environmental controls for temperature, humidity, lighting, fire, and power) will be 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, controlled interface equipment, and communications equipment).

Scalability-related considerations—

- Security controls will be scalable by the size and complexity of the particular organization implementing the controls and the impact level of the information system. Scalability addresses the breadth and depth of security control implementation.[9] Discretion is needed in scaling the security controls to the particular environment of use to ensure a cost-effective, risk-based approach to security control implementation.

Risk-related considerations—

- Security controls that uniquely support the confidentiality, integrity, or availability security objectives can be downgraded to the corresponding control in a lower baseline (or appropriately modified or eliminated if not defined in a lower baseline) if, and only if, the downgrading action: (i) is consistent with the FIPS Publication 199 security categorization for the corresponding security objectives of confidentiality, integrity, or availability before moving to the high water mark;[10] (ii) is supported by an organizational assessment of risk; and (iii) does not affect the security-relevant information within the information system.[11]

[8] For example, while the baseline security controls require identification and authentication of organizational personnel who maintain and support information systems that provide public access services, the same controls might not be required for users accessing those systems through public interfaces to obtain publicly available information. On the other hand, identification and authentication must be required for users accessing information systems through public interfaces to access their private/personal information.

[9] For example, a contingency plan for a large and complex organization with a moderate-impact or high-impact information system may be quite lengthy and contain a significant amount of implementation detail. In contrast, a contingency plan for a smaller organization with a low-impact information system may be considerably shorter and contain much less implementation detail.

[10] When employing the "high water mark" concept, some of the security objectives (i.e., confidentiality, integrity, or availability) may have been increased to a higher impact level. As such, the security controls that uniquely support these security objectives will have been upgraded as well. Consequently, organizations must consider appropriate and allowable downgrading actions to ensure cost-effective, risk-based application of security controls.

[11] Information that is security-relevant at the system level (e.g., password files, network routing tables, cryptographic key management information) must be 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. Organizations must exercise caution in downgrading confidentiality or integrity-related security controls to ensure that the downgrading action does not affect the security-relevant information within the information system.

Compensating Security Controls

Compensating security controls are the management, operational, or technical controls employed by an organization in lieu of prescribed controls in the low, moderate, or high security control baselines, which provide equivalent or comparable protection for an information system. Compensating security controls for an information system will be employed by an organization only under the following conditions: (i) the organization selects the compensating controls from the security control catalog in NIST Special Publication 800-53; (ii) the organization provides a complete and convincing rationale and justification for how the compensating controls provide an equivalent security capability or level of protection for the information system; and (iii) the organization assesses and formally accepts the risk associated with employing the compensating controls in the information system. The use of compensating security controls must be reviewed, documented in the system security plan, and approved by the authorizing official for the information system.

Organization-Defined Security Control Parameters

Security controls in NIST Special Publication 800-53 containing organization-defined parameters (i.e., assignment or selection operations) give organizations the flexibility to define selected portions of the controls to support organization-unique requirements or objectives. After the application of the scoping guidance and consideration of compensating controls, organizations will review the list of security controls with variable parameters and assign appropriate values. Where specified, minimum and maximum values must be adhered to unless further restricted by applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures, or are indicated by a risk assessment in order to adequately protect the information system and the operations and assets of the organization. For example, a security control requiring the conduct of awareness training at least annually, may be further restricted by the implementing organization based on the considerations cited above, to require more frequent training.

Supplementing the Security Control Baselines

The security control baselines listed in NIST Special Publication 800-53 will be viewed as foundations or starting points in the selection of adequate security controls for organizational information systems. The security control baselines provide, for classes of information systems (derived from FIPS 199 security categorizations), the minimum level of *due diligence* demonstrated by an organization toward the protection of its operations and assets and for satisfying the minimum security requirements set forth in this standard. The final determination of the set of security controls necessary for adequate security depends on the organization's assessment of risk. In many cases, additional or enhanced security controls will be needed to address specific threats to and vulnerabilities in the information system or to satisfy the requirements of applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures. The security control catalog in NIST Special Publication 800-53 facilitates the process of enhancing security controls or adding controls to the security control baselines. The techniques and methodologies used by organizations in supplementing the security control baselines are beyond the scope of this standard.

APPENDIX A TERMS AND DEFINITIONS

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

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

AGENCY: Any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the government (including the Executive Office of the President), or any independent regulatory agency, but does not include: (i) the Government Accounting Office; (ii) the Federal Election Commission; (iii) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or (iv) government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities. [44 U.S.C., SEC. 3502]

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

AUTHORIZING OFFICIAL: Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. *Synonymous with Accreditation Authority.*

AVAILABILITY: Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]

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

CHIEF INFORMATION OFFICER: 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. [44 U.S.C., Sec. 5125(b)]

CHIEF INFORMATION SECURITY OFFICER: See Senior Agency Information Security Officer.

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

COMPENSATING CONTROLS: The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization under strict terms and conditions in lieu of the prescribed security controls in the low, moderate, or high security control baselines, that provide equivalent or comparable protection for an information system.

CONFIDENTIALITY: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]

CONTROLLED INTERFACE: Mechanism that facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system). [CNSS Instruction 4009]

COUNTERMEASURES: Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. [CNSS Instruction 4009] *Synonymous with security controls and safeguards.*

ENVIRONMENT: Aggregate of external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system. [CNSS Instruction 4009]

EXECUTIVE AGENCY: 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. [41 U.S.C., SEC. 403]

FEDERAL AGENCY: See Agency.

FEDERAL INFORMATION SYSTEM: 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. [40 U.S.C., SEC. 11331]

HIGH-IMPACT SYSTEM: 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: 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.

INFORMATION: An instance of an information type. [FIPS Publication 199]

INFORMATION OWNER: Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. [CNSS Instruction 4009]

INFORMATION RESOURCES: Information and related resources, such as personnel, equipment, funds, and information technology. [44 U.S.C., SEC. 3502]

INFORMATION SECURITY: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [44 U.S.C., SEC. 3542]

INFORMATION SYSTEM: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [44 U.S.C., SEC. 3502]

INFORMATION SYSTEM OWNER: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. [CNSS Instruction 4009 Adapted]

INFORMATION TECHNOLOGY: 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. [40 U.S.C., SEC. 1401]

INFORMATION TYPE: 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. [FIPS Publication 199]

INTEGRITY: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]

LOW-IMPACT SYSTEM: 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.

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

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

MODERATE-IMPACT SYSTEM: 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 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: 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. [44 U.S.C., SEC. 3542]

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

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

POTENTIAL IMPACT: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect, a serious adverse effect, or a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. [FIPS Publication 199]

RECORDS: The recordings of evidence of activities performed or results achieved (e.g., forms, reports, test results) which serve as the 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). [NIST Special Publication 800-53]

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

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

SAFEGUARDS: 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. [CNSS Instruction 4009 Adapted] *Synonymous with security controls and countermeasures.*

SANITIZATION: Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs. [CNSS Instruction 4009 Adapted]

SCOPING GUIDANCE: Specific factors related to technology, infrastructure, public access, scalability, common security controls, and risk that can be considered by organizations in the applicability and implementation of individual security controls in the security control baseline.

SECURITY CATEGORY: 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. [FIPS Publication 199]

SECURITY CONTROLS: 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. [FIPS Publication 199]

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

SECURITY OBJECTIVE: Confidentiality, integrity, or availability. [FIPS Publication 199]

SECURITY PLAN: See System Security Plan.

SECURITY REQUIREMENTS: Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or 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: 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. [44 U.S.C., Sec. 3544]

SYSTEM: See information system.

SYSTEM SECURITY PLAN: 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. [NIST Special Publication 800-18]

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

THREAT: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. [CNSS Instruction 4009 Adapted]

THREAT SOURCE: 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.*

USER: Individual or (system) process authorized to access an information system. [CNSS Instruction 4009]

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

APPENDIX B REFERENCES

[1] Committee for National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, May 2003.

[2] E-Government Act of 2002 (Public Law 107-347), December 2002.

[3] Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

[4] Federal Information Security Management Act of 2002 (Public Law 107-347, Title III), December 2002.

[5] Information Technology Management Reform Act of 1996 (Public Law 104-106), August 1996.

[6] National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005.

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

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

[9] Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Security of Federal Automated Information Resources*, November 2000.

[10] Paperwork Reduction Act of 1995 (Public Law 104-13), May 1995.

[11] Privacy Act of 1974 (Public Law 93-579), September 1975.

APPENDIX C ACRONYMS

CIO	Chief Information Officer
CNSS	Committee for National Security Systems
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
USC	United States Code