March 2006

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

MINIMUM SECURITY REQUIREMENTS FOR FEDERAL INFORMATION AND INFORMATION SYSTEMS: FEDERAL INFORMATION PROCESSING STANDARD (FIPS) 200 APPROVED BY THE SECRETARY OF COMMERCE

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

The Secretary of Commerce, Carlos M. Gutierrez, has approved a new Federal Information Processing Standard (FIPS) to improve the security of government information and information systems. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, which was approved on March 9, 2006, assists federal agencies in conducting effective information security programs and in meeting the requirements of the Federal Information Security Management Act (FISMA) of 2002.

FISMA requires all federal agencies to develop, document, and implement agency-wide information security programs and to provide information security for the information and information systems that support the operations and assets of the agency, including those systems provided or managed by another agency, contractor, or other source. To help agencies carry out these policies, FISMA called for NIST to develop federal standards for the security categorization of federal information and information systems according to risk levels, and for minimum security requirements for information and information systems in each security category. FIPS 199, *Standards for the Security Categorization of Federal Information and Information Systems*, issued in February 2004, was the first standard that was specified by FISMA. FIPS 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.

FIPS 200, which is the second standard that was specified by FISMA, is an integral part of the risk management framework that NIST has developed to assist federal agencies in providing appropriate levels of information security based on levels of risk. In applying the provisions of FIPS 200, agencies will categorize their systems as required by FIPS 199, and then select an appropriate set of security controls from NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, to satisfy their minimum security requirements.

Security controls are the management, operational and technical safeguards and countermeasures needed to protect the confidentiality, integrity, and availability of a computer system and its information. Management safeguards range from risk assessments to security planning. Operational safeguards include factors such as personnel security and basic hardware/software maintenance.

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since April 2005:

Who We Are
The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

Technical safeguards include items such as audit trails and communications protection.

Applicability of FIPS 200

FIPS 200 is applicable to:

● 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

● all federal information systems other than those information systems designated as national security systems as defined in 44 US Code Section 3542(b)(2).

FIPS 200 was 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 the standard.

Using FIPS 200

In applying FIPS 200, federal agencies must first categorize their information systems as low-impact, moderate-impact, or high- impact for the security objectives of confidentiality, integrity, and availability in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*. A low-impact system is an information system in which all three of the security objectives for confidentiality, integrity, and availability 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. A high-impact system is an information system in which at least one security objective is high. This 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.

Specifying Minimum Security Requirements

FIPS 200 specifies minimum security requirements for federal information and information systems in seventeen security-related areas that represent a broad-based, balanced information security program. The seventeen security-related areas encompass the management, operational, and technical aspects of protecting federal information and information systems, and include the following:

Access control: limiting information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems), and to types of transactions and functions that authorized users are permitted to exercise.

Audit and accountability: creating, protecting, and retaining information system audit records that are needed for the monitoring, analysis, investigation, and reporting of unlawful, unauthorized or inappropriate information system activity, and ensuring that the actions of individual users can be traced so that the individual users can be held accountable for their actions.

Awareness and training: ensuring that managers and users of information systems are made aware of the security risks associated with their activities and of applicable laws, policies, and procedures related to security, and ensuring that personnel are trained to carry out their assigned information security-related duties.

Certification, accreditation, and security assessments: assessing security controls for effectiveness, implementing plans to correct deficiencies and to reduce vulnerabilities, authorizing the operation of information systems and system connections, and monitoring system security controls.

Configuration management: establishing baseline configurations and inventories of systems, enforcing security configuration settings for products, monitoring and controlling changes to baseline configurations and to components of systems throughout their system development life cycles.

Contingency planning: establishing and implementing plans for emergency response, backup operations, and post-disaster recovery of information systems.

Identification and authentication: identifying and authenticating the identities of users, processes, or devices that require access to information systems.

Incident response: establishing operational incident handling capabilities for information systems, and tracking, documenting, and reporting incidents to appropriate officials.

Maintenance: performing periodic and timely maintenance of systems, and providing effective controls on the tools, techniques, mechanisms, and personnel that perform system maintenance.

Media protection: protecting information in printed form or on digital media, limiting access to information to authorized users, and sanitizing or destroying digital media before disposal or reuse.

Personnel security: ensuring that individuals in positions of authority are trustworthy and meet security criteria, ensuring that information and information systems are protected during personnel actions, and employing formal sanctions for personnel failing to comply with security policies and procedures.

Physical and environmental protection: limiting physical access to systems and to equipment to authorized individuals, protecting the physical plant and support infrastructure for systems, providing supporting utilities for systems, protecting systems against environmental hazards, and providing environmental controls in facilities that contain systems.

Planning: developing, documenting, updating, and implementing security plans for systems.

Risk assessment: assessing the risk to organizational operations, assets, and individuals resulting from the operation of information systems, and the processing, storage, or transmission of information.

Systems and services acquisition: allocating resources to protect systems, employing system development life cycles processes, employing software usage and installation restrictions, and ensuring that third-party providers employ adequate security measures to protect outsourced information, applications, or services.

System and communications protection: monitoring, controlling and protecting communications at external and internal boundaries of information systems, and employing architectural designs, software development techniques, and systems engineering principles to promote effective security.

System and information integrity: identifying, reporting, and correcting information and system flaws in a timely manner, providing protection from malicious code, and monitoring system security alerts and advisories.

Selection of Security Controls

Organizations must meet the minimum security requirements by selecting the appropriate security controls and assurance requirements that are described in SP 800-53, *Recommended Security Controls for Federal Information Systems*. This publication was originally issued in February 2005 and was updated through June 2005. To keep the security controls discussed in the publication up to date with current practices, NIST conducts an annual review and update process. The purpose of the annual review is to ensure that the security controls listed in the control catalog and that the specified minimum security controls represent the current state of the practice in safeguards and countermeasures for information systems.

In March 2006, NIST announced that it had revised SP 800-53 and made it available for public review and comment as Draft SP 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*. During the year after the original publication of SP 800-53, NIST received many thoughtful comments about the format, structure, and content of the publication. The revision reflects customer experience gained from employing the security controls and security controls baselines, changing security requirements within organizations, and new technologies that are available for information security.

FIPS 200 and its supporting publication SP 800-53 establish conditions to enable organizations to be flexible in tailoring their security control baselines. Agencies may, for example, apply appropriate scoping guidance, taking into consideration the issues related to the specific technologies employed by the agency, the common security controls employed, requirements for public access to information systems, specific physical conditions, the size and complexity of systems, and the risks involved. Guidance is provided on how to assess these considerations in implementing agency security controls. SP 800-53 also provides guidance on the use of compensating security controls that may be employed by an organization in lieu of the prescribed controls in the low, moderate, or high security control baselines. Other areas of flexibility for

agencies include defining selected portions of the controls to support organization-unique requirements or objectives, and supplementing the security control baselines with additional controls that may be needed.

Other Guidance Supporting the Implementation of FIPS 199 and FIPS 200

NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, assists organizations in developing security plans that summarize the security requirements for each information system, and the security controls in place or planned for meeting the requirements. The publication relates the security planning processes that agencies should employ to the requirements of FIPS 199 and FIPS 200.

NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, is being revised to be consistent with NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. The revision will add information about FIPS 199, compensating controls, common controls, SP 800-53 and SP 800-53A, and agency security program-level assessments (including a program-level questionnaire). The system-level questionnaire will be used as a reporting form for the seventeen security-related areas that are listed above.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, provides guidance to organizations in identifying the risks to their information systems, assessing the risks, and taking steps to reducing the risks to an acceptable level. The risk management process enables organizations to protect the information systems that store, process, and transmit organizational information, to make well-informed risk management decisions, and to apply system authorization and accreditation processes.

NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, provides guidance for the security certification and accreditation of information systems. Security certification and accreditation are important activities that support a risk management process, and are essential to an organization's information security program. Security accreditation is 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, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. Security certification, which supports the accreditation process, is a comprehensive assessment 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 of the system.

NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, assists federal agencies in identifying information types and information systems and assigning impact levels for confidentiality, integrity, and availability. The impact levels are based on the security categorization definitions in FIPS 199 and are included in two volumes. Volume I of SP 800-60 provides guidelines for identifying impact levels by type and suggests impact levels for administrative and support information common to multiple agencies. Volume II includes the rationale for information type and impact level recommendations and examples of recommendations for agency-specific, mission-related information.

Other publications, directives, and policies that support compliance with FISMA are available from the FISMA Implementation Project website listed below.

Schedule for Implementation of FIPS 200

FIPS 200 is effective immediately, and agencies are expected to be in compliance within one year. Agencies will have one year to implement the security controls included in SP 800-53 after the current review period has been completed, and the publication has been issued in final form. However, agencies are encouraged to initiate compliance activities immediately.

For More Information

Information about the FISMA Implementation Project, including references, contacts, and information about upcoming conferences and workshops, is available on the NIST website: http://csrc.nist.gov/sec-cert.

FIPS 199 and FIPS 200 are available on the NIST website: http://csrc.nist.gov/publications/fips/index.html.

NIST Special Publications are available on the NIST website: http://csrc.nist.gov/publications/nistpubs/index.html.