March 2004

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

FEDERAL INFORMATION PROCESSING STANDARD (FIPS) 199, STANDARDS FOR SECURITY CATEGORIZATION OF FEDERAL INFORMATION AND INFORMATION SYSTEMS

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

A new Federal Information Processing Standard (FIPS), recently approved by the Secretary of Commerce, will help federal agencies protect the information and information systems that support their operations and assets. FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, is an important component of a suite of standards and guidelines that NIST is developing to improve the security in federal information systems, including those systems that are part of the nation's critical infrastructure. (See listing of these planned publications at the end of this bulletin.)

FIPS 199 will enable agencies to meet the requirements of the Federal Information Security Management Act (FISMA) and improve the security of federal information systems. The security standard will also make it possible for federal agencies to establish priorities for protecting their information systems, ranging from very sensitive, mission-critical operations to lower-priority systems performing less critical operations. Background information on NIST's efforts to provide the security standards, guidelines, and technical tools for implementing FISMA is available at: http://csrc.nist.gov/sec-cert/ca-background.html.

FIPS 199 was approved after an open public review and comment process that included notices published in the *Federal Register* and posted on the NIST website. Comments and recommendations were received from more than thirty individuals and groups. The new FIPS 199 is available electronically at: http://csrc.nist.gov/publications/fips.

Applicability of FIPS 199

FIPS 199 is effective immediately and applies 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 United States Code Section 3542(b)(2).

Why Security Categorization Standards Are Needed

FISMA, Title III of the E-Government Act of 2002 (Public Law 107-347), was passed by the one hundred and seventh Congress and signed into law by the President in December 2002. This legislation recognizes the importance of information security to the economic and national security interests of the United States, and tasked NIST with responsibilities for standards and guidelines, including the development of:

- Standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;

Continued on page 2

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 November 2002

- *Security for Telecommuting and Broadband Communications*, November 2002
- *Security of Public Web Servers*, December 2002
- *Security of Electronic Mail*, January 2003
- *Secure Interconnections for Information Technology Systems*, February 2003
- *Security for Wireless Networks and Devices*, March 2003
- *ASSET: Security Assessment Tool for Federal Agencies*, June 2003
- *Testing Intrusion Detection Systems*, July 2003
- *IT Security Metrics*, August 2003
- *Information Technology Security Awareness, Training, Education, and Certification*, October 2003
- *Network Security Testing,* November 2003
- *Security Considerations in the Information System Development Life Cycle*, December 2003
- *Computer Security Incidents: Assessing, Managing, and Controlling the Risks*, January 2004

- ❑ Guidelines recommending the types of information and information systems to be included in each category; and
- ❑ Minimum information security requirements (i.e., management, operational, and technical controls) for information and information systems in each such category.

By providing a common framework and method for categorizing information and information systems, FIPS 199 responds to the first task assigned to NIST. Use of this standard will enable agencies to identify and prioritize their most important information and information systems by defining the maximum impact a breach in confidentiality, integrity, or availability could have on the agency's operations, assets, and/or individuals.

A FIPS 199 security categorization serves as the starting point for the selection of security controls for an agency's information system—controls that are commensurate with the importance of the information and information system to the agency. Additional NIST guidance will instruct agencies how to use FIPS 199 to select minimum security controls for an information system and subsequently assess the controls 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. The standard also promotes more effective management, oversight, and expenditure of agency information security resources and more consistent reporting on the agency's security accomplishments to the Office of Management and Budget (OMB) and to the Congress. Future NIST standards and guidelines will focus on the second and third tasks above.

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/.

A Risk-Based Approach

FISMA and earlier legislation, the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), provide for a risk-based approach to information security. OMB provides guidance in its Circular A-130, Appendix III, on carrying out the risk-based approach and requires agencies to:

- ❑ Plan for adequate security of each information system as part of the agency management and planning processes,
- ❑ Ensure that appropriate officials are assigned responsibilities for security,
- ❑ Periodically review the security controls in their information systems, and
- ❑ Authorize system processing prior to operations, and periodically thereafter.

The objective is to conduct agency operations and accomplish agency missions with *adequate security* or security commensurate with risk, considering threats, vulnerabilities, value of the information system or application, and the effectiveness of current or proposed security controls. The risk-based approach should be applied throughout the System Development Life Cycle (SDLC).

Security Objectives, Impact Levels, and Security Categorization

FIPS 199 is predicated on a simple and well-established concept—determining appropriate priorities for agency information systems and subsequently applying appropriate measures to adequately protect those systems. The security controls applied to a particular information system should be commensurate with the system's criticality and sensitivity. FIPS 199 assigns this level of criticality and sensitivity, called *security categorization*, to information and information systems based on potential impact on agency operations (mission, functions, image, or reputation), agency assets, or individuals should there be a breach in security due to the loss of confidentiality (i.e., unauthorized disclosure of information), integrity (i.e., unauthorized modification of information), or availability (i.e., denial of service).

In FIPS 199, confidentiality, integrity, and availability are defined as *security objectives* for information and information systems:

- ❑ **Confidentiality:** "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" A loss of confidentiality is the unauthorized disclosure of information.
- ❑ **Integrity:** "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" A loss of integrity is the unauthorized modification or destruction of information.
- ❑ **Availability:** "Ensuring timely and reliable access to and use of information…" A loss of availability is the disruption of access to or use of information or an information system.

For each type of information that is processed, stored, or transmitted by an information system and for the information system itself, FIPS 199 requires assigning a security category to the information and information system. The security category consists of an impact level for each of the three security objectives of confidentiality, integrity, and availability. An impact level of low (L), moderate (M), or high (H) represents the impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals should there be a breach in security in the respective security objective areas (i.e., for each security objective area, the impact level could be L, M, or H). The assignment of security categories must take place within the context of each organization and the overall national interest.

Impact levels are defined in FIPS 199 as follows:

The potential impact is **low** if the loss of confidentiality, integrity, or availability could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect could mean that the loss of confidentiality, integrity, or availability might:

- Cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
- Result in minor damage to organizational assets, minor financial loss, or minor harm to individuals.

The potential impact is **moderate** if the loss of confidentiality, integrity, or availability could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect could mean that the loss of confidentiality, integrity, or availability might:

- Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
- Result in significant damage to organizational assets, significant financial loss, or significant harm to individuals, but not loss of life or serious life threatening injuries.

ITL Bulletins Via E-Mail
We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

The potential impact is **high** if the loss of confidentiality, integrity, or availability could be expected to have a *severe* or *catastrophic* adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect could mean that the loss of confidentiality, integrity, or availability might:

- Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
- Result in major damage to organizational assets, major financial loss, or severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Security Categorization Applied to Information Types and Information Systems

The security category of an information type that is processed, stored, or transmitted by an information system can be associated with both user information and system information, and can be applicable to information in either electronic or non-electronic form. System information such as network routing tables, password files, and cryptographic key management information must always be protected at a level that is appropriate for the most critical or sensitive user information.

In establishing the appropriate security category of an *information type*, organizations should determine the potential impact for each security objective associated with the particular information type. For example, an organization might determine that there is low potential impact from a loss of confidentiality of its public information, that there is a moderate potential impact from a loss of integrity, and that there is a moderate potential impact from a loss of availability. FIPS 199 provides examples of how to determine and to express the security categories of information types.

In establishing the appropriate security category of an *information system*, organizations should consider the security categories of all information types that are processed, stored, or transmitted on the information system. For a system, the potential impact values assigned to the respective security objectives of confidentiality, integrity, and availability should be the highest values from among those security categories that have been determined for each type of information processed. For example, an organization might determine the security category for sensitive contract information in a system used for acquisitions is moderate (for confidentiality), moderate (for integrity), and low (for availability). The organization might also determine that security category for routine administrative information processed on the same system is low (for confidentiality), low (for integrity), and low (for availability). The security category for the information system should be expressed in terms of the maximum potential impact values for each security objective from the various information types resident on the acquisition system. In this example, the system's security category would be moderate (for confidentiality), moderate (for integrity), and low (for availability).

System Development Life Cycle and Future Standards and Guidelines

Employed within the System Development Life Cycle (SDLC), FIPS 199 can be used as part of an agency's risk management program to help ensure that appropriate security controls are applied to each information system and that the controls are adequately assessed to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the system security requirements. The following activities, consistent with NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, can be applied to both new and legacy information systems within the SDLC—

- ***Categorize*** the information system (and the information resident within that system) based on a FIPS 199 impact analysis (See NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, for guidance in assigning security categories and refining the impact analysis).

- □ ***Select*** an initial set of security controls for the information system (as a starting point) based on the FIPS 199 security categorization (See NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, or FIPS 200, *Security Controls for Federal Information Systems*, which will replace NIST Special Publication 800-53 in December 2005 in fulfillment of the FISMA legislative requirement for mandatory minimum security requirements for federal information systems.)
- □ ***Refine*** the initial set of security controls selected for the information system based on local conditions including agency-specific security requirements, specific threat information, cost-benefit analyses, the availability of compensating controls, or other special circumstances.
- □ ***Document*** the agreed-upon set of security controls in the security plan for the information system including the agency's rationale and justification for any refinements or adjustments to the initial set of controls (See NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*).
- □ ***Implement*** the security controls in the information system. For legacy systems, some or all of the security controls selected may already be in place.
- □ ***Assess*** the security controls using appropriate assessment 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. (See NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, summer 2004).
- □ ***Determine*** the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the planned or continued operation of the information system (See NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*).
- □ ***Authorize*** system processing (or for legacy systems, authorize continued system processing) if the level of risk to the agency's operations, assets, or individuals is acceptable to the authorizing official (See NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*).
- □ ***Monitor*** selected security controls in the information system on an continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate agency officials on a regular basis (See NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*).

Since some of the documents referenced above are either in development or planned at the time this bulletin was published, the reader should consult: http://www.csrc.nist.gov for up-to-the minute progress reports on the FISMA program and related guidance documents.

Disclaimer:
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.