November 2004

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

## UNDERSTANDING THE NEW NIST STANDARDS AND GUIDELINES REQUIRED BY FISMA

### How Three Mandated Documents are Changing the Dynamic of Information Security for the Federal Government

*By Ron Ross and Patricia Toth, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology*

The Federal Information Security Management Act (FISMA) of 2002 places significant requirements on federal agencies, including the National Institute of Standards and Technology (NIST), for the protection of information and information systems. In response to this important legislation, NIST is leading the development of key information system security standards and guidelines as part of its FISMA Implementation Project. This high-priority project includes the development of security categorization standards, standards and guidelines for the specification, selection, and testing of security controls for information systems. The flagship standard among those being developed by NIST is Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, published in February 2004. This mandatory standard, applicable to non-national security systems as defined by FISMA, introduces some significant changes in how the U.S. Government protects its information and information systems, including those systems that comprise the nation's critical infrastructure.

To gauge the impact of FIPS 199 on the massive inventory of federal information systems, one must first understand how the world of information technology has changed over the past two decades. Not long ago, the information systems that populated federal enterprises consisted of large, expensive, standalone mainframes, taking up a significant amount of physical space in the facilities and consuming substantial portions of organizational budgets. Information systems were viewed as "big ticket items" requiring specialized policies and procedures to effectively manage.

Today, information systems are more powerful, less costly (for the equivalent computational capability), networked, and ubiquitous. The systems, in most cases, are viewed by agencies as commodity items, although items coupled more tightly than ever to the accomplishment of agency missions. However, as the technology raced ahead and brought a new generation of information systems into the federal government with new access methods and a growing community of users, some of the policies, procedures, and approaches employed to ensure the protection of those systems did not keep pace.

### The Problem with the Old Way of Doing Business – Establishing Priorities

The administrative and technological costs of offering a high degree of protection for all federal information systems at all times would be prohibitive, especially in times of tight governmental budgets. Achieving adequate, cost-effective information system security (as defined in Office of Management and Budget Circular A-130, Appendix III) in an era where information technology is a commodity requires some fundamental changes in how the protection problem is addressed. Information systems must be assessed to establish priorities based on the importance of those systems to agency missions.

There is clearly a criticality and sensitivity continuum with regard to agency information systems that affects the

*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 October 2003

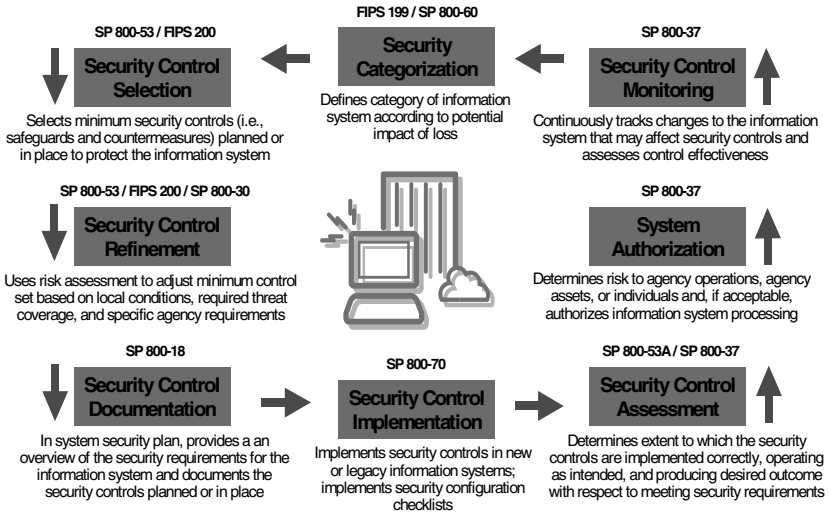
ultimate prioritization of those systems. At one end of the continuum, there are high-priority information systems performing very sensitive, mission-critical operations, perhaps as part of the critical information infrastructure. At the other end of the continuum, there are low-priority information systems performing routine agency operations. The application of safeguards and countermeasures (i.e., security controls) to all these information systems should be tailored to the individual systems based on established agency priorities (i.e., where the systems fall on the continuum of criticality/sensitivity with regard to supporting the agency's missions). The level of effort dedicated to testing and evaluating the security controls in federal information systems and the determination and acceptance of risk to the mission in operating those systems (i.e., security certification and accreditation) should also be based on the same agency priorities.

Until recently, there were a limited number of standards and guidelines available to help agencies implement a more granular approach to establishing security priorities for their information systems. The result—many agencies would end up expending too many resources (both administratively and technologically) to protect information systems of lesser criticality/sensitivity and not enough resources to protect systems of greater criticality/sensitivity. Some "load balancing" was needed.

**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/.

**Risk Management Framework**




## Ushering in a New Era with FIPS 199

FIPS 199, the mandatory federal security categorization standard approved by the Secretary of Commerce, provides the first step toward bringing some order and discipline to the challenge of protecting the large number of information systems supporting the operations and assets of the federal government. The standard 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 based on the 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). FIPS 199 requires federal agencies to do a "triage" on all of their information types and systems, categorizing each as low, moderate, or high impact for the three security objectives of confidentiality, integrity (including authenticity and non-repudiation), and availability.

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 (SP) 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 SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, for guidance in assigning security categories.)
- ***Select*** an initial set of security controls for the information system (as a starting point) based on the FIPS 199 security categorization. (See NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. Note: FIPS 200, *Minimum Security Controls for Federal Information Systems*, will replace NIST SP 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 organization-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 system security plan including the organization's justification for any refinements or adjustments to the initial set of controls. (See NIST SP 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 methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (See NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, initial public draft, fall 2004.)
- ***Determine*** the risk to organizational operations and assets resulting from the planned or continued operation of the information system. (See NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.)
- ***Authorize*** information system processing (or for legacy systems, authorize continued system processing) if the level of risk to the agency's operations or assets is acceptable to the authorizing official. (See NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.)
- ***Monitor*** selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate agency officials on a regular basis. (See NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.)

Significant changes to the information system or the security requirements for that system may prompt the agency to revisit the above activities. Examples of significant changes to an information system include, but are not limited to, installation of a new or upgraded operating system, middleware component, or application; modifications to systems ports, protocols, or services; installation of a new or upgraded hardware platform or firmware component; or modifications to cryptographic modules or services. Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system.

**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 Benefits to Agency Security Programs

The long-term effect of employing a FIPS 199 standards-based approach is more targeted, more cost-effective, and improved security for federal information and information systems. While the interconnection of information systems often increases the risk to an agency's operations and assets, FIPS 199 and the associated suite of standards and guidelines provide a common framework and understanding for expressing information security, and thus promote greater consistency across diverse organizations in managing that risk. Agencies will determine which information systems are the most important to accomplishing assigned missions based on the security categorization of those systems and will protect the systems appropriately. Agencies will also determine which systems are the least important to their missions and will not allocate excessive resources for the protection of those systems.

In the current high technology era where information systems are viewed as commodities and are routinely used to protect some of the nation's most important assets within the federal government and the critical infrastructure, FIPS 199 is a standard that is right for the time. In the end, the new security standard, when properly applied, will facilitate a more effective allocation of available resources for protecting information systems, determine the need and provide a justification for the allocation of additional resources, and result in a substantial improvement in the security posture of the government's information systems.

The FISMA-related security standards and guidelines discussed in this ITL bulletin are available at the FISMA Implementation Project website at http://csrc.nist.gov/sec-cert.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900