ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

RECOMMENDED SECURITY CONTROLS FOR FEDERAL INFORMATION SYSTEMS: GUIDANCE FOR SELECTING COST-EFFECTIVE CONTROLS USING A RISK-BASED PROCESS

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

Security controls are the management, operational, and technical safeguards that protect the confidentiality, integrity, and availability of an information system and its information. Organizations face critical decisions in selecting and implementing the right controls and in making the controls an effective part of their information security programs. The Information Technology Laboratory at the National Institute of Standards and Technology (NIST) has developed guidance to help organizations protect their information and information systems and to use security controls that are selected through a risk-based process.

Development of NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*

The basic questions that organizations should address when selecting security controls are: What controls are needed to protect systems, while supporting their operations and safeguarding their assets? Can the selected controls be implemented? And once implemented, are they effective? NIST SP 800-53, *Recommended Security Controls for Federal Information Systems,* helps organizations to answer these questions and to maintain effective information security programs. This ITL Bulletin summarizes the special publication.

Written by Ron Ross, Stuart Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, George Rogers, and Annabelle Lee, NIST SP 800-53 was developed using input from a variety of sources including published NIST standards and guidance, Department of Defense (DoD) policies, international standards, and other federal government directives and policies. SP 800-53 provides guidance for federal agencies that operate federal information systems other than those systems designated as national security systems, as defined in 44 U.S.C., Section 3542. However, the security controls that are specified in NIST SP 800-53 are complementary to similar guidance that has been issued for national security systems.

NIST SP 800-53 was issued in final form in February 2005 after extensive public input and review. The authors received many valuable comments from government and private sectors that helped to shape the final recommendations. While primarily aimed toward helping federal agencies achieve more secure information systems, other activities including state, local and tribal governments, and private sector organizations should find the guide useful in selecting and specifying security controls for their information and information systems.

Understanding and Selecting Security Controls

Recommended Security Controls for Federal Information Systems provides a foundation for understanding the fundamental concepts of security controls. The introductory material presents the concept of security controls and their use within a well-defined information security program. Some of the issues discussed include the structural components of controls, how the controls are organized into families, and the use of controls to support information security programs. The guide outlines the essential steps that should be followed to determine needed controls, to assure the effectiveness of controls, and to main-

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 March 2004

- *Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems*, March 2004
- *Selecting Information Technology Security Products*, April 2004
- *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004
- *Information Technology Security Services: How to Select, Implement, and Manage*, June 2004
- *Guide for Mapping Types of Information and Information Systems to Security Categories*, July 2004
- *Electronic Authentication: Guidance For Selecting Secure Techniques*, August 2004
- *Information Security Within The System Development Life Cycle*, September 2004
- *Securing Voice Over Internet Protocol (IP) Networks*, October 2004
- *Understanding the New NIST Standards and Guidelines Required by FISMA*, November 2004
- *Integrating IT Security into the Capital Planning and Investment Control Process*, January 2005
- *Personal Identity Verification (PIV) of Federal Employees and Contractors: Federal Information Processing Standard (FIPS) 201 Approved by the Secretary of Commerce*, March 2005
- *Implementing The Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, April 2005

tain the effectiveness of installed controls. A detailed process for selecting and specifying appropriate security controls is described.

The publication's appendices provide additional resources including general references, definitions, explanation of acronyms, a breakdown of security controls for graduated levels of security requirements, a catalog of security controls, and information relating security controls to other standards and control sets. The controls in the catalog are organized into classes of operational, management, and technical controls, and then into families within each class. NIST plans to review and to update the controls in the catalog as technology changes and as new safeguards and new information security countermeasures are identified.

NIST SP 800-53 is available in electronic format from the NIST Computer Security Resource Center at http://csrc.nist.gov/publications/nistpubs/index.html.

NIST SP 800-53 and FISMA Requirements

NIST SP 800-53 is one of the series of standards and guidelines that NIST has developed to help federal agencies implement their responsibilities under the Federal Information Security Management Act (FISMA). FISMA requires that all federal agencies develop, document, and implement agency-wide information security programs to protect 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 support agencies in conducting their information security programs, the FISMA directed NIST to develop:

- Standards for categorizing information and information systems 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 199, *Standards for Security Categorization of Federal Information and Information Systems*, issued in February 2004, addresses the first task specified by FISMA. FIPS 199 requires that agencies categorize their information systems as low-impact, moderate-impact, or high-impact systems for the security objectives of confidentiality, integrity, and availability. In a low-impact system, all security objectives are low. If at least one of the security objectives is moderate and no security objective is greater than moderate, the system is moderate-impact. A high-impact system is one for which at least one security objective is high. This categorization is the first step in the agency's risk management process, to be followed by the selection of security controls that are appropriate for the impact levels determined in the categorization procedure.

Draft FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems,* which is in the final stages of development, will specify a risk-based approach for agencies to follow in determining their minimum security requirements and for selecting cost-effective security controls. NIST expects to announce FIPS 200 for public review and comment in the near future. In applying the provisions of proposed FIPS 200, agencies will categorize their systems as required by FIPS 199, and then select an appropriate set of security controls from NIST SP 800-53. These controls are the foundation for the selection of adequate controls, but the final determination of the appropriate set of controls depends upon the organization's assessment of risk.

Implementing an Effective Information Security Program

To maintain an effective information security program that protects their information and information systems, organizations should follow a systematic process to carry out these tasks:

- Periodically assess the risks that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization;
- Adopt policies and procedures that are based on risk assessments, reduce risks cost-effectively to an acceptable level, and ensure that information security is addressed throughout the life cycle of the information system;
- Develop plans to provide information security for networks, facilities, information systems, or groups of information systems;
- Provide security awareness training to educate personnel about information security risks and responsibilities for following policies and procedures that are designed to reduce risks;
- Periodically test and evaluate the effectiveness of information security policies, procedures, practices, and security controls;
- Use an organizational process to plan, implement, evaluate, and document remedial actions that address identified deficiencies;
- Adopt procedures that detect, report, and respond to security incidents; and
- Support plans and procedures to ensure continuity of operations.

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.

A Risk-Based Approach to Selecting Controls

In adopting a risk-based approach to the selection of security controls, organizations should consider the effectiveness and efficiency needed in their systems, and the requirements that are specified in applicable, laws, directives, executive orders, policies, standards, and regulations. The following activities can be applied to new and legacy information systems within the context of overall life-cycle planning, including the planning guides in the System Development Life Cycle and the Federal Enterprise Architecture:

- Categorize information systems and their information based on the procedures for categorizing systems that are detailed in FIPS 199. Based on the security categorization, select an initial set of security controls from the catalog of controls listed in Appendix D of SP 800-53.
- Adjust the initial set of security controls based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses, the availability of compensating controls, or special circumstances.
- Document the agreed-upon set of security controls, taking into account any adjustments or refinements.

The Security Control Catalog

The security controls listed in the SP 800-53 catalog represent the current state-of-the-practice safeguards and countermeasures for information systems. These controls will be revised and extended as experience is gained in using the controls, and as requirements and technology change.

The security controls should be considered as the foundations or starting points in the selection of controls for low-impact, moderate-impact, and high-impact information systems, based on categorizations done in accordance with FIPS 199. Since the determination of adequate controls is based on the organization's determination of risk, additional controls may be needed to address specific threats or particular organizational requirements.

The security controls cover the following seventeen areas:

- Risk assessment – including policies and procedures; security categorization; and management of the risk assessment process.
- Certification, accreditation, and security assessments – including policies and procedures; control of system connections; management of the accreditation process; and assessments and monitoring of controls.
- System services and acquisition – including policies and procedures; management of resource allocation, life cycle support, acquisitions, and system documentation; and control of software usage and of outsourced information services.
- Security planning – including policies and procedures; development and implementation of plans; and management of staff behavior rules and privacy procedures.
- Configuration management – including policies and procedures; management of information system components; and control and management of changes to information systems and to system settings.
- System and communications protection – including policies and procedures; application partitioning; controls for denial of service protection, resource use, boundary protection, and telecommunications services; and management of cryptography applications and public key infrastructure certificates.
- Personnel security – including policies and procedures; and management of staff positions, screening, terminations, and transfers.
- Awareness and training – including policies and procedures; and management of the content of training and of training records.
- Physical and environmental protection – including policies and procedures; management of access authorizations; controls for access to transmission facilities and display media; management of access logs and visitor controls; and management of power equipment, cabling, lighting, fire protection, and alternate work sites.
- Media protection – including policies and procedures; processes for media access, labeling, storage, transport, and sanitization; and destruction and disposal of media.
- Contingency planning – including policies and procedures; contingency training; and development, maintenance, and testing of plans; management of alternate processing sites, telecommunications services, and information backup; and management of system recovery.
- Maintenance – including policies and procedures; management of periodic maintenance; and control of maintenance tools and maintenance personnel.
- System and information integrity – including policies and procedures; management of flaw protection, malicious code protection, and intrusion detection; controls for security alerts, and for software and information integrity; spam and spyware protection; and error handling.
- Incident response – including policies and procedures; incident training, testing, handling, monitoring, and reporting.

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/.

- Identification and authentication – including policies and procedures; management of devices, identifiers, and authenticators; and management of cryptographic processes.
- Access control – including policies and procedures; access enforcement; information flow enforcement; management of login attempts; system use notification; remote access controls; and wireless access controls.
- Accountability and audit – including policies and procedures; audit processing; audit monitoring, analysis, and reporting; and audit report generation.

Using Security Controls to Improve Information System Security

NIST SP 800-53 provides detailed information about these seventeen categories of broadly applicable security controls and helps organizations select the controls that are appropriate for a wide variety of security requirements. When correctly implemented and periodically assessed for effectiveness, security controls can contribute to organizational confidence that requirements for the security of information systems are being met. The controls are a starting point for risk assessments and play an important role in the organization's practices for comprehensive system security planning and life cycle management.

The extensive reference list in SP 800-53 includes standards, guidelines, and recommendations that organizations can use for their comprehensive security planning and life cycle management processes. These publications can be accessed from the NIST web pages at http://csrc.nist.gov/.

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.*

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

Official Business
Penalty for Private Use $300

Address Service Requested

PRSRT STD
POSTAGE & FEES PAID
NIST
PERMIT NUMBER G195