January 2007

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

SECURITY CONTROLS FOR INFORMATION SYSTEMS: REVISED GUIDELINES ISSUED BY NIST

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

The National Institute of Standards and Technology (NIST) Information Technology Laboratory recently updated its guidance to federal agencies for selecting and specifying security controls for their information systems. Security controls are the management, operational, and technical safeguards or countermeasures that protect the confidentiality, integrity, and availability of an information system and its information.

The revised NIST guidance assists federal agencies in selecting an appropriate set of security controls for their information systems, in accordance with standards and requirements specified by the Federal Information Security Management Act (FISMA) of 2002. Using the tailoring guidance provided in the revised publication, agencies will have flexibility in selecting and adjusting the security controls that they specify in order to meet their specific mission requirements and their operational needs in a cost-effective manner.

NIST Special Publication (SP) 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*

NIST SP 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*, was written by Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, and George Rogers, and published by NIST in December 2006. The publication, when used with other standards and guidelines, assists federal agencies in protecting the information systems that support federal government operations and assets.

NIST SP 800-53 presents the fundamental concepts concerning the selection and specification of security controls. The topics discussed include the structural components of security controls and how the controls are organized into families of controls; the baseline, or minimum, controls that can be selected; the common controls that can be applied in more than one organizational information system; the controls needed to protect systems in exchanges with external information systems; implementation of controls within an information system with assurance that the controls are effective; and NIST's plans for periodic review of the controls and maintenance of a catalog of effective controls.

The guide describes the recommended comprehensive process that organizations should follow for selecting and specifying security controls for an information system. Topics covered include the steps that an organization should take to manage risks; the requirement for federal agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability; how to select and tailor an initial set of minimum, or baseline, controls; how to supplement the tailored baseline controls to achieve needed security protections; and how to update controls through regular reviews as part of a risk management process.

The appendices to NIST SP 800-53 provide extensive information about the selection and specification of security controls. Included are a list of references, a glossary of terms used in the publication,

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 February 2006:

and a list of acronyms. One table lists the catalog of minimum security controls in summarized form and indicates the appropriate control and any applicable control enhancements that would be needed to protect low-impact, moderate-impact, and high-impact information systems.

Another part of the appendix explains the minimum assurance requirements for the security controls listed in the catalog, and provides supplemental guidance concerning how the minimum requirements are to be applied. One large section of the appendix provides a catalog of security controls organized into families with supplemental guidance and with information associated with each control to allow for the enhancement of the control. Mappings of the relationships of security controls to government and voluntary industry standards and to other control sets, mappings of the relationships of security controls to NIST standards and guidelines, and guidance on the application of controls to industrial control systems complete the appendices.

The security controls guide is available on NIST's web pages at:

http://csrc.nist.gov/publications/nistpubs/index.html.

Supplemental Publications

In addition to the final version of NIST SP 800-53 available on the above web page, you will also find supplemental publications to assist in the selection and specification of security controls. NIST SP 800-53 introduces the concept of baseline controls, which are the initial security controls recommended for an information system, based on the system's security categorization. (See section on FISMA below.) Tailoring guidance in NIST SP 800-53 can be applied to the initial control set to produce a tailored baseline. This tailored security control baseline is the starting point for organizations to determine the appropriate safeguards and countermeasures necessary to protect their information systems. Supplements to the tailored baseline may be needed based on the organization's operational needs and its assessment of risk.

Annex 1 to NIST SP 800-53 provides a summary of baseline security controls for low-impact information systems. It also provides control enhancements, full descriptions of the controls and enhancements, and the minimum assurance requirements for low-impact information systems. Annex 2 contains similar information for moderate-impact systems, and Annex 3 covers high-impact systems.

Other available documents are marked-up versions of NIST SP 800-53 that indicate changes made to initial public drafts including a document that summarizes all of the changes that were made to the February 2005 version of the guide in the development of the December 2006 version.

Establishing an Integrated Information Security Program

Security controls should be selected and used as part of a well-defined and documented information security program. To be effective, an information security program should provide for:

* Periodic assessments of risk to evaluate the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems.

* Development of policies and procedures that are based on assessments of risk and that reduce the risks to an acceptable level and address information security throughout the life cycle of each information system.

* Plans to provide adequate information security for networks, facilities, information systems, or groups of systems.

* Security awareness training for personnel, including contractors and other users of information systems, about the risks associated with their activities and their responsibilities for implementing policies and procedures for information security.

* A process for planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies.

* Procedures for detecting, reporting, and responding to security incidents; and

* Plans and procedures for continuity of operations.

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.

Federal Information Security Management Act (FISMA)

The Federal Information Security Management Act (FISMA) requires that all federal agencies develop, document, and implement agency-wide information security programs and 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 designated NIST to develop federal standards for the security categorization of federal information and information systems according to risk levels, and 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 NIST developed to meet FISMA requirements. 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, *Minimum Security Requirements for Federal Information and Information Systems*, which was approved on March 9, 2006, is the second standard that was specified by FISMA. After agencies have categorized their systems in accordance with FIPS 199, they are required to determine minimum security requirements for seventeen security-related areas, and to select an appropriate set of security controls to satisfy the minimum requirements. Security controls, which are specified in NIST SP 800-53, are organized to match the seventeen security-related areas that are identified in FIPS 200. The application of controls is an essential component of a broad-based, balanced information security program.

For more information about activities that support the FISMA Implementation Project, see NIST's web page at http://csrc.nist.gov/sec-cert/index.html.

Using NIST SP 800-53, Revision 1, in the Risk Management Process

Risk management is an essential part of an organization's information security program, providing an effective framework for the selection of appropriate security controls. The risk-based approach 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.

The risk management process includes the following steps:

* **Categorize** the information system and its information in accordance with FIPS 199.

* **Select** an initial set of baseline, or minimum, controls from NIST SP 800-53, based on the categorization and the minimum security requirements defined in FIPS 200. Apply the tailoring guidance from NIST SP 800-53 to identify the starting point controls.

* **Supplement** the initial set of tailored security controls based on the assessment of risk and the organization's specific requirements.

* **Document** the security controls, including refinements and adjustments to the initial set of controls, in the system security plan.

* **Implement** the security controls in the information system, and apply security configuration settings.

* **Assess** the security controls to determine if implemented correctly, operating properly, and meeting security requirements.

* **Authorize** information system operation, using security certification and accreditation procedures. Security accreditation is the decision to authorize operation of an information system and to accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. Security certification is a comprehensive assessment of the system's security controls to determine the extent to which the controls are implemented correctly, operating as intended, and meeting the security requirements of the system.

* **Monitor** and assess selected security controls to track changes to the information system on a continuous basis, and reassess the effectiveness of controls.

NIST standards and guides that assist organizations in using the risk management process to select security controls are listed in the More Information section below.

Changes to Controls Selection Process in NIST SP 800-53, Revision 1

NIST SP 800-53, Revision 1, used in conjunction with FIPS 200, provides federal organizations with options for significant flexibility in their selection and specification of security controls. The tailoring guidance introduced in the guide will enable federal agencies to eliminate unnecessary controls, to incorporate compensating controls when needed, and to specify agency specific conditions. This approach gives agencies flexibility to respond to known threats and to take action on agency-identified risks. The guide reinforces requirements for agencies to consider the potential organizational and national-level impacts when they categorize their information systems as low-impact, moderate-impact, or high-impact systems.

Organizations are advised to select common controls for information systems whenever possible. The advantages of common controls are cost-effectiveness and consistency of implementation. Common controls should be developed, implemented, and continuously monitored by a central management team, and the results of security assessments should be shared with all information system owners. Within the common control structure, controls may be tailored to be system-specific and be described in system security plans.

Other changes relate to instituting controls that are appropriate for the use of information services obtained from external service providers. Agencies should establish trust relationships with the providers to assure that the external information systems have implemented necessary and effective security controls. Also changes were made to the security certification, security accreditation, user identification and authentication, media labeling, media storage, and media transport security controls. All of these changes are identified in the document available on the NIST web page, summarizing the changes that were made in Revision 1 of NIST SP 800-53.

More Information

NIST publications that support the risk management process and the selection, implementation, and assessment of security controls include:

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, 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, *Minimum Security Requirements for Federal Information and Information Systems*, specifies minimum security requirements for federal information and information systems in

seventeen security-related areas that represent a broad-based, balanced information security program.
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 identify the security controls in place or planned for meeting the requirements.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, provides guidance to organizations in identifying the risks to their missions brought about by the use of information systems, assessing the risks, and taking steps to reduce the risks to an acceptable level.

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 in support of the risk management process.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, provides guidance in selecting, specifying, and tailoring security controls that will provide an appropriate level of security, based on the organization's assessment of mission risk.

NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, will enable organizations to develop an effective assessment plan. The guide, which is currently available in draft form, is expected to be completed in mid-2007.

NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, provides a checklist that enables organizations to determine if their systems should be designated national security systems in accordance with FISMA.

NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, assists organizations in identifying information types and impact levels, and assigning impact levels for confidentiality, integrity, and availability. The impact levels are based on the security categorization definitions in FIPS 199.

NIST SP 800-70, *Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers*, describes NIST's program to facilitate the development and use of security configuration checklists.

NIST publications assist organizations in planning and implementing a comprehensive approach to information security. For information about NIST standards and guidelines that are listed above, as well as other security-related publications that support the goals of FISMA, see NIST's web page:

http://csrc.nist.gov/publications/index.html

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.

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.