REVISED CATALOG OF SECURITY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS: FOR USE IN BOTH NATIONAL SECURITY AND NONNATIONAL SECURITY SYSTEMS

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

The Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST) recently revised and expanded its catalog of security controls to help organizations protect their information and information systems. Developed by the Interagency Working Group of the Joint Task Force Transformation Initiative, the revised catalog brings together, for the first time, comprehensive information about security controls that can be used in both national security and nonnational security information systems. The cooperative development of the catalog represents an ongoing effort to build a unified information security framework for the federal government and its contractors. The Joint Task Force includes participants from the Department of Defense, the intelligence community, and civil agencies of the federal government.

The updated catalog, NIST Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations,* incorporates updated effective practices for information security. These best practices provide broad-based and comprehensive safeguards and countermeasures for protecting today's information systems. The uniform approach to describing controls for both national security and nonnational security applications helps all government organizations address the advanced cyber threats that can exploit vulnerabilities in federal information systems. A common foundation for information security also provides a strong basis for reciprocal acceptance of information system interconnection and facilitates information sharing.

Security Controls in Information Security Programs

Security controls are the management, operational, and technical safeguards or countermeasures that an organization employs to protect the confidentiality, integrity, and availability of its information systems and its information. Organizations select, implement, and assess their security controls most effectively when the process is carried out as part of a comprehensive and documented information security program. The foundation for this integrated approach is the system development life cycle, a multistep process that starts with the initiation, analysis, design, and implementation of a system and continues through the maintenance and disposal of the system.

The selection, implementation, and evaluation of security controls are important components of the risk-based approach to the management of information systems. Risk management is the process that information technology managers apply to balance the operational and economic costs of protective measures for their information and

information systems with the gains in capabilities and improved support of their organizational missions that result from the use of efficient protection procedures.

NIST has developed a six-step Risk Management Framework to help organizations manage risks from the use of information systems. The framework includes a series of steps for identifying and maintaining an appropriate set of security controls to reduce risks to an acceptable level by:

- **Categorizing** the information system and the information being processed, stored, and transmitted by the system, based on the potential impact to the organization should events occur to put the system and its information at risk;
- **Selecting** an appropriate set of security controls for the information system after determining the security categorizations;
- **Implementing** the security controls in the information system;
- **Assessing** 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;
- **Authorizing** information system operation based upon a determination of the risk to organizational operations, organizational assets, or to individuals resulting from the operation of the information system and the determination that the risk is acceptable; and
- **Monitoring** and assessing selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the changes, and reporting the security status of the system to appropriate organization officials on a regular basis.

Information about the Risk Management Framework and the NIST publications that support organizations in managing the risks associated with their information systems is available from the NIST Web page http://csrc.nist.gov/groups/SMA/fisma/framework.html.

The July issue of the ITL Bulletin included a description of the Risk Management Framework and provided links to resources that are useful in the risk management process. The bulletin is available at the NIST Web page: http://csrc.nist.gov/publications/nistbul/july2009_risk-management-framework.pdf.

Federal Agency Responsibilities to Select and Specify Security Controls

The Federal Information Security Management Act (FISMA) of 2002 establishes a governmentwide policy for the implementation and assessment of security controls. FISMA requires that federal agencies develop, document, and implement programs to protect their information and information systems. This policy applies to the systems that support the operations and assets of the agency, and includes those systems provided or managed by another agency, contractor, or other source. FISMA calls for agencies to

apply a risk-based policy to achieve cost-effective results for the security of their information and information systems.

Standards and guidelines developed by NIST help agencies to carry out effective information security programs based on the management of risk. Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems,* specifies that federal organizations categorize their information and information systems, based on the potential impact on the organization should adverse events occur which could jeopardize the information and information systems needed by the organization to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

Under FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems,* organizations use the categorization results obtained under FIPS 199 to designate their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. For each information system, agencies then select an appropriate set of security controls from NIST SP 800-53, *Recommended Security Controls for Federal Information System and Organizations,* to satisfy their minimum security requirements.

NIST Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal information Systems and Organizations,* replaces an earlier version of the catalog. Revision 3 is part of a larger strategic initiative to focus on enterprise-wide, near real-time risk management; that is, managing risks from information systems in dynamic environments of operation that can adversely affect organizational operations and assets, individuals, other organizations, and the Nation.

Aimed toward achieving more secure information systems and more effective risk management programs for the federal government, NIST SP 800-53 facilitates using a consistent and repeatable approach in selecting and specifying security controls for information systems and organizations. The catalog of security controls helps organizations to fulfill their current requirements for implementing protection measures, and to meet the challenges of future needs for protection.

The Joint Task Force Transformation Initiative considered security controls from a variety of sources in developing the revised catalog. These sources included security controls from the defense, audit, financial, healthcare, and intelligence communities as well as controls defined by national and international standards organizations. The Task Force’s goal was to produce a group of security controls to address a broad range of security requirements for information systems and organizations. The controls are consistent with and complementary to other established information security standards.

NIST SP 800-53, Revision 3, is available from the NIST Web page

http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf.

Information Presented in NIST SP 800-53, Revision 3

The publication starts with basic information on the selection and specification of security controls, including the structural components of security controls and how the controls are organized into families. There are three general classes of security controls: management, operational, and technical.

The concept of baseline security controls is discussed. Baseline controls, which are the starting point for the selection of security controls, are chosen based on the security category and the associated impact level of the information system that are determined in accordance with FIPS 199 and FIPS 200. Baseline controls, which are included in Appendix D (see below) and which can be adjusted in accordance with the guidance provided in NIST SP 800-53, comprise the minimum set of security controls for the information system. Although the baseline is intended to be the starting point for the selection of controls, organizations have flexibility in applying the baseline security controls. Organizations can tailor the security control baseline so that it is more closely aligned with their mission, business requirements, and environments of operation. Through their risk assessment processes, agencies can validate the selection of security controls and determine if any additional controls are needed to protect the agency's operations, taking into consideration the agency's mission, functions, and other factors.

Other topics discussed in NIST SP 800-53 are the use of common security controls to support organization-wide information security programs and the use of security controls when external services are used. External services, which are implemented outside the organization, are not part of the organization's information systems. Many organizations rely on external providers for essential services that are needed to carry out their missions and business functions. Federal organizations are responsible for and accountable for the risk incurred by the use of external services. This risk can be addressed through the implementation of compensating controls when necessary.

NIST SP 800-53 discusses the need for assurance that the security controls implemented within an information system are effective in their application. Organizations can achieve assurance through the actions taken by developers, implementers, and operators in the specification, design, development, implementation, operation, and maintenance of security controls. Assurance is also achieved through the actions taken by security control assessors 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.

A chapter of the publication focuses on how to select and specify security controls for an organizational information system. Organizations are advised to:

- apply the organization's approach to managing risk;
- categorize the information system and determine the system impact level in accordance with FIPS 199 and FIPS 200;

- select security controls, including tailoring the initial set of baseline security controls;
- supplement the tailored baseline as necessary based on an organizational assessment of risk; and
- assess the security controls as part of a comprehensive continuous monitoring process.

Supporting information for the controls is contained in the appendices to the publication. Appendix A provides a reference list that includes applicable laws, policies, directives, regulations, memoranda, standards and guidelines. Appendix B provides users with definitions for security terminology used within the publication, and Appendix C contains acronyms used within the publication.

Appendix D contains the security control baselines that represent the starting point in determining the security controls for low-impact, moderate-impact, and high-impact information systems, as defined in FIPS 200.

Appendix E lists the minimum assurance requirements for security controls described in the security control catalog. The assurance requirements are directed at the activities and actions that the developers and implementers of security controls define and apply to increase the level of confidence that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. The assurance requirements are applied on a control-by-control basis.

Appendix F provides the extensive range of safeguards and countermeasures for organizations and information systems. Each control of the three general classes (management, operational, technical) is described. The descriptive structure includes a control section providing an explanation of the control capabilities needed to protect information or a particular aspect of an information system. This section also includes specific security-related activities or actions to be carried out by the organization or by the information system. Other components of the descriptive structure are supplemental guidance on applying the control, and enhancements for building in additional functionality to a control and increasing the strength of a control. A reference section and information on priority and baseline allocations complete the structure.

Appendix G describes information security program management (PM) controls which complement the security controls in Appendix F and focus on the organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs. Organizations specify the individuals who are responsible for the development, implementation, assessment, authorization, and monitoring of the information security program management controls. Program management controls are documented in the organization’s information security program plans. The organization’s overall information security program plan supplements the individual security plans developed for each organizational information system. Together, the security plans for the

individual information systems and for the information security program cover the full range of security controls that are employed by the organization.

Appendix H includes mapping tables that help organizations compare their security controls to the controls specified in an international standard, ISO/IEC 27001 (International Organization for Standardization/International Electrotechnical Commission), *Information technology–Security techniques–Information security management systems–Requirements.* Appendix I includes security controls, enhancements, and supplemental guidance for industrial control systems.

NIST Plans for Maintaining SP 800-53 and Related Publications

The security controls included in NIST SP 800-53 will be carefully reviewed and revised periodically to reflect the experiences gained from using the controls, changing security requirements, emerging threats, vulnerabilities and attack methods, and the availability of new technologies. While the security controls will change as conditions change, any proposed additions, deletions or modifications to the catalog will be announced and open to public review and comments to solicit government and private sector opinions and to build consensus for any changes. NIST plans to maintain stable, yet flexible and technically rigorous security controls in the catalog.

NIST will continue to work with the national and nonnational security communities in updating other key publications that will reflect the joint approach to information security. These publications and their planned revised titles include:

- NIST SP 800-30, *Guide for Conducting Risk Assessments*;
- NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach;*
- NIST SP 800-39, *Integrated Enterprise-wide Risk Management: Organization, Mission, and Information Systems View*; and
- NIST SP 800-53A, *Guide for Assessing Security Controls in Federal Information Systems and Organizations.*

The schedule for the development of these and other FISMA-related publications based on new milestones established by the participating partners in the Joint Task Force Transformation Initiative can be found at http://csrc.nist.gov/groups/SMA/fisma/schedule.html.

Information on NIST Publications

For information about NIST standards and guidelines that are referenced in this bulletin, as well as other security-related publications, see NIST's Web page http://csrc.nist.gov/publications/index.html. Past ITL bulletins covering the use of security controls, risk management issues, and the application of NIST standards and guidelines can be found on at http://csrc.nist.gov/publications/PubsITLSB.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.