December 2003

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

SECURITY CONSIDERATIONS IN THE INFORMATION SYSTEM DEVELOPMENT LIFE CYCLE

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

When do you have to pay attention to the security requirements of your information system? From the very earliest stages of planning for the development of the system to its final disposal is the advice of the National Institute of Standards and Technology (NIST). By considering security early in the information system development life cycle (SDLC), you may be able to avoid higher costs later on and develop a more secure system from the start.

NIST's Information Technology Laboratory recently issued Special Publication (SP) 800-64, *Security Considerations in the Information System Development Life Cycle*, by Tim Grance, Joan Hash, and Marc Stevens, to help organizations include security requirements in their planning for every phase of the system life cycle, and to select, acquire, and use appropriate and cost-effective security controls. The guide discusses the selection of a life cycle model by the organization and the responsibilities of the organization's managers and staff members for conducting the system development process. While NIST SP 800-64 describes security and a generic system development life cycle for illustrative purposes, the basic concepts can be applied, with tailoring, to any SDLC model or acquisition method the organization is using.

The appendices to the guide contain sample documents to help federal organizations during the system acquisition process. These include a standard format for requests for proposals (RFPs); specifications, tasks, and clauses that can be incorporated into RFPs to acquire information security features; and examples of contract language for specific information security measures. This ITL Bulletin summarizes NIST SP 800-64, which is available at http://csrc.nist.gov/publications/nistpubs/index.html.

The System Development Life Cycle (SDLC)

The system development life cycle starts with the initiation of the system planning process, and continues through system acquisition and development, implementation, operations and maintenance, and ends with disposition of the system. Specific decisions about security must be made in each of these phases to assure that the system is secure.

Initiation Phase

The initiation phase begins with a determination of need for the system. The organization develops its initial definition of the problem that could be solved through automation. This is followed by a preliminary concept for the basic system that is needed, a preliminary definition of requirements, and feasibility and technology assessments. Also during this early phase, the organization starts to define the security requirements for the planned system. Management approval of decisions reached is important at this stage.

The information developed in these early analyses will be used to estimate the costs for the entire life cycle of the system, including information system security. An investment analysis should be performed to determine the appropriate strategy for achieving the system requirements, while taking mission needs and budget constraints into account. Expenditures for security should be considered before the system is built. It is difficult to add functionality into a system after it has been built, and it is usually more cost-

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 8901, Gaithersburg, MD 20899-8901, 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 September 2002

❒ *Cryptographic Standards and Guidelines: A Status Report*, September 2002

❒ *Security Patches and the CVE Vulnerability Naming Scheme: Tools to Address Computer System Vulnerabilities*, October 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 effective to include preventive security measures from the start rather than to deal with security breaches later on.

During this initiation phase, the organization establishes the security categorization and conducts a preliminary risk assessment for the planned information system. Categorization of the information system using federal standards and guidelines aids system security planners in defining information system security according to levels of impact, and in selecting a baseline of initial security controls for those impact levels. Security categories are then used in conjunction with vulnerability and threat information in assessing risk to an organization.

- Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, should be used by federal organizations to determine the security category for the information system. FIPS 199 defines three levels of potential impact on organizations or on individuals should certain adverse events occur. These are events that could jeopardize the information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information to assess the risk that an organization incurs when operating an information system and to select appropriate security controls. FIPS 199 is available as a pre-publication final document at http://csrc.nist.gov/.
- A **preliminary risk assessment** should be performed to develop a brief initial description of the basic security needs of the system, including needs to protect the integrity, availability, and confidentiality of system information. The preliminary risk assessment should define the threat environment in which the system will operate and the potential vulnerabilities. This assessment should be followed by an initial identification of required security controls that will protect the system in its operational environment. A detailed risk assessment is developed in the next phase.

Acquisition / Development Phase

In this phase, the organization should conduct a **requirements analysis,** which draws on and expands the work done in the Initiation phase. This in-depth study of the organization's need for the system should analyze the security aspects of the system requirements.

- A **formal risk assessment** identifies threats to and vulnerabilities in the information system, the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability would have on agency assets or operations, and the security controls that are needed. This analysis builds on the initial risk assessment performed during the Initiation phase, but is more detailed and specific. The risk assessment brings together important information about the protection of the information system, and it generates information required for the security plan. This risk assessment should be conducted before the approval of design specifications. The assessment should consider existing controls and their effectiveness, as well as the impact that the new system might have on other systems to which it will be directly or indirectly connected. Enterprise security architectures can help minimize the vulnerabilities that might be introduced by the new system.
- The **security functional requirements analysis** considers the system security environment, including the enterprise information security policy and the enterprise security architecture. The analysis should address all requirements for confidentiality, integrity, and availability of information, and should include a review of all legal, functional, and other security requirements contained in applicable laws, regulations, and guidance.
- The **security assurance requirements analysis** addresses the activities and assurance needed to produce the desired level of confidence that the information security will work correctly and effectively. This analysis, based on legal and functional security requirements, should be used to determine how much and what kinds of assurance are required. The goal is to achieve cost-effective assurance that meets the requirements for protecting the organization's information assets. Tests and evaluations, such as the following, can provide information about system quality and support confidence in the system.

The **Common Criteria for IT Security Evaluation,** contained in International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15408, is used to evaluate information security products to support user confidence that the products meet defined security claims. NIST and the National Security Agency jointly manage the National Information Assurance Partnership (NIAP), which develops comprehensive security requirements and security specifications for key technologies and evaluates the security features of products in accordance with the Common Criteria. Commercial testing laboratories conduct the evaluations after being accredited by NIST's National Voluntary Laboratory Accreditation Program (NVLAP). A list of evaluated products is available at http://niap.nist.gov/cc-scheme/ValidatedProducts.html.

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/.

NIST conducts the **Cryptographic Module Validation Program (CMVP)**, which also uses independent, accredited laboratories to perform conformance testing of cryptographic modules for conformance to Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, and other federal cryptographic algorithm standards. Established jointly by NIST and the Communications Security Establishment (CSE) of the Government of Canada, the CMVP tests products to assure that the federal cryptographic algorithms have been correctly implemented in the modules. Federal agencies that have determined that they need cryptographic methods to protect their information must use validated products. A list of validated products is available at http://csrc.nist.gov/cryptval/.

Third-party and other evaluations can be used, but the objectivity of these evaluations must be considered. Government organizations may conduct their own evaluations. The results of these evaluations may or may not be published and are normally not considered to be endorsements by federal agencies. Other sources of evaluations include trade, professional, and commercial organizations.

- ❑ **Consideration and reporting** of development cost enable organizations to determine how much of the development cost can be attributed to information security over the life cycle of the system. These costs include hardware, software, personnel, and training. The best source of this data is the risk assessment, which identifies the controls that will mitigate vulnerabilities, and includes a cost-benefit analysis of recommended controls based on consideration of the possibility of an incident and its potential impact. When the controls have been selected, the cost of each can be determined. OMB Circular A-11, Part 3, requires that federal organizations report this information for their major acquisitions.

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 **security plan** ensures that the planned or existing security controls are fully documented. The security plan also provides a complete description of the information system, and provides references to key documents supporting the organization's information security program: the configuration management plan, contingency plan, incident response plan, security awareness and training plan, rules of behavior, risk assessment, security test and evaluation plan, system interconnection agreements, security authorizations and accreditations, and the plan of action with milestones.
- ❑ A study of **security controls** focuses on the controls described in the security plans to assure that they are designed, developed, and implemented. Additional controls may be needed for information systems currently in operation.
- ❑ A **security test and evaluation plan** should be developed for the security controls that can be evaluated prior to deployment. The controls must be tested and evaluated for correct implementation and effectiveness. Controls of a non-technical activity, such as management and operational controls, cannot be tested and evaluated until the information system is deployed.
- ❑ **Other planning processes,** studies, evaluations, and contract specifications associated with the development and acquisition process, involving appropriate staff members, help to assure that the security requirements of the system are identified and achieved. The IT security experts should work with the contracting office to select the most advantageous type of contract. A team or group of participants from functional areas such as legal, human resources, information security, and physical security can provide useful perspectives in reviewing the plans. Involvement of appropriate staff early in the planning process can help to reduce life-cycle costs and make it easier to change requirements early on.

Implementation Phase

In this phase, the system is installed and evaluated in the organization's operational environment.

- ❑ **Inspection and acceptance** of the delivered system is necessary to verify that the functionality described in the specifications has been included in the deliverables. Testing can be done by the organization or by an independent contractor to assure that the system meets the specifications, and that the security features are operating.
- ❑ **Security controls are integrated** at the site where the system is to be deployed for operation. Security control settings and switches are enabled in accordance with vendor instructions and available security implementation guidance.
- ❑ OMB Circular A-130, Appendix III, requires that the system be certified and accredited before it is operational. Information about the **certification and accreditation** process is available from http://csrc.nist.gov/sec-cert/. Federal agencies should periodically test and evaluate the security controls in their information systems to assure effective implementation, using established verification techniques and procedures. **Security certification** gives organization officials confidence that the appropriate safeguards and countermeasures are in place. Security certification also uncovers and describes the known vulnerabilities in the information system. This

information helps officials make decisions about **security accreditation,** which is an authorization for a system to operate. Granted by a senior organization official, accreditation is based on the verified effectiveness of security controls to some agreed-upon level of assurance and an acceptance of identified residual risk to agency assets or operations. The decision is risk-based and is supported by testing and evaluation results produced during the security control verification process.

Operations / Maintenance Phase

In this phase of the SDLC, information systems are operating, and may undergo enhancements and modifications. Hardware and software may be added or replaced. The system is monitored for continued performance in accordance with user requirements, and needed system modifications are incorporated. The operational system is periodically assessed to determine how it can be made more efficient and effective. Operations continue as long as the system can be effectively adapted to respond to the organization's changing needs.

- ❑ **Configuration management and control** procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system and subsequently to controlling and maintaining an accurate inventory of any changes to the system. Changes to the hardware, software, or firmware of a system can have a significant impact on the security of the system. System changes should be documented, and their potential impact on security should be assessed regularly.
- ❑ Controls must be **continuously monitored** through periodic testing and evaluation to assure that they are effective in their application. Monitoring of security controls verifies the continued effectiveness of those controls and reports on the security status of the system's information.

Disposition Phase

This phase provides for disposal and/or contract closeout of the system (for contracts that were employed during the earlier phases). Disposal of the system may involve a separate contract. Government resources and assets must be protected when information systems are transferred, disposed of, or no longer usable. For some systems, there may not be a definitive end to the SDLC since the system may evolve or transition to the next generation of technology, as a result of changing requirements. System security plans should be modified to evolve with the system.

- ❑ **Information should be retained** to conform to current legal requirements and to accommodate future technology changes that might make the system's data retrieval method obsolete. The environmental, management, and operational information about a system may be relevant and useful in developing the security plan for the follow-on system. The data processed by the system should be preserved for use in a follow-on system or archived in accordance with applicable regulations and policies.
- ❑ Data should be deleted, erased, and written over as necessary, and the **media** that stored the data should be **sanitized**. Degaussing, overwriting, and media destruction are some of the methods that may be used.
- ❑ **Disposal of the hardware and software** should be completed at the direction of the information system security officer.

More Information

The following Special Publications (SPs) provide help to organizations in planning, developing, operating, maintaining, and terminating secure information systems. These publications are available in electronic format from the NIST Computer Security Resource Center at http://csrc.nist.gov/publications.

For a complete list of references, consult NIST SP 800-64.

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, provides guidance on the fundamentals of information system security.

NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, discusses developing and updating security plans.

NIST SP 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, discusses the concept of assurance.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, discusses the risk-based approach to security and provides guidance on conducting risk assessments.

NIST SP 800-31, *Intrusion Detection Systems (IDS),* and NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*, provide information on using and deploying IDSs and firewalls.

NIST SP 800-35, *Guide to Information Technology Security Services*, covers evaluating, selecting, and managing security services throughout the life cycle.

NIST SP 800-42, *Guidelines on Network Security Testing*, describes available security testing techniques, their strengths and weaknesses, and the recommended frequencies for testing as well as strategies for deploying network security testing.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, provides recommended security controls based on system impact level (available as a draft at http://csrc.nist.gov/publications/drafts.html).

Information about Federal Information Processing Standards (FIPS), including FIPS-approved algorithms and cryptographic modules that must be used by federal agencies, is available at http://csrc.nist.gov/publications/fips/index.html.

Office of Management and Budget documents that cover life cycle planning issues include OMB Circular A-11, Part 3, "Planning, Budgeting, and Acquisition of Capital Assets, and OMB Memorandum 00-07, "Incorporating and Funding Security in Information Systems Investments."

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