ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

INFORMATION TECHNOLOGY SECURITY SERVICES: HOW TO SELECT, IMPLEMENT, AND MANAGE

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

Organizations often need expert assistance in maintaining and improving the security of their information technology (IT) systems. Whether they get this assistance from internal sources or from commercial vendors of security services, organizations must review and evaluate the sources before committing to service agreements. A carefully managed process can help assure that sound decisions are made and that system security is strengthened.

Guide to Information Technology Security Services

NIST's Information Technology Laboratory recently published NIST Special Publication (SP) 800-35, *Guide to Information Technology Security Services, Recommendations of the National Institute of Standards and Technology*, which provides guidance to help organizations negotiate the many complexities and challenges in selecting information technology security services. Written by Tim Grance, Joan Hash, Marc Stevens, Kristofor O'Neal, and Nadya Bartol, NIST SP 800-35 helps those who are responsible for selecting, implementing, and managing their organization's IT security services. NIST recommends that organizations adopt systematic evaluation and decision processes to guide their selection of IT security services and to satisfy their security requirements. This *ITL Bulletin* summarizes the new IT services selection guide.

The foundation for the selection of IT security services is a comprehensive information security management program, including risk management procedures that are applied throughout the System Development Life Cycle (SDLC). This same process also underlies the selection of IT security products, the focus of our April 2004 *ITL Bulletin* covering NIST SP 800-36, *Guide to Selecting Information Technology Security Products*.

NIST SP 800-35 discusses the roles and responsibilities of the people within an organization who select, implement and manage the security services life cycle. It provides an overview of the security services life cycle and describes the issues to be addressed concerning security services. Examples of specific services are described. The appendices include lists of references and acronyms, an outline of a security services provider agreement, sample acquisition language, and answers to frequently asked questions.

The services selection guide is available in electronic format from the NIST Computer Security Resource Center at http://csrc.nist.gov/publications. When used with other NIST publications, including those listed in the More Information section at the end of this bulletin, the guide will help organizations develop a comprehensive approach to organizing their overall IT security efforts, managing risks, and using IT security services.

People Responsible For Security Services

The people responsible for selecting, implementing, and managing services within an organization will vary depending upon the type and scope of the service needed, the service arrangement, and the size of the organization. Larger organizations that use external security service providers extensively will have different requirements and more people involved than smaller organizations with more limited requirements.

The people who may be involved in the process include the following:

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 February 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
- *Security Considerations in the Information System Development Life Cycle*, December 2003
- *Computer Security Incidents: Assessing, Managing, and Controlling the Risks*, January 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

- Chief Information Officer, who is responsible for the organization's IT planning, budgeting, investment, performance, and acquisition;
- Contracting Officer, who has authority to enter into, administer, and terminate contracts;
- Contracting Officer's Technical Representative, who is appointed by the Contracting Officer to manage the technical aspects of a particular contract;
- IT Investment Board (or equivalent), which is responsible for planning and for managing the capital planning and investment control process for federal agencies, as specified in the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act);
- IT Security Program Manager, who is responsible for developing enterprise standards for IT security, coordinating and performing system risk analyses, analyzing alternatives for minimizing risks, and supporting the acquisition of appropriate security solutions;
- IT System Security Officer, who is responsible for ensuring the security of an information system throughout its life cycle;
- Program Manager, who owns the data, initiates the procurement, is involved in strategic planning and is aware of functional services requirements;

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/.

- Privacy Officer, who assures that the service and service arrangement meet privacy policies regarding the protection, dissemination, and disclosure of information; and/or
- Other participants, who may include the system certifier and accreditor, system users, and people representing information technology, configuration management, design, engineering, and facilities groups.

IT Security Life Cycle

The SDLC provides the framework that enables the IT security decision makers to organize their IT security efforts—from initiation to closeout. The systematic management of the IT security services process fits into this framework. The organization's IT security is critically dependent upon the careful consideration of the many issues connected to security services, and to the prudent management of organizational risks. IT security decision makers must think about the costs involved and the underlying security requirements, as well as the potential impact of their decisions on the organizational mission, operations, strategic functions, personnel, and service provider arrangements.

The selection, implementation, and management of security services are included in the following six phases of the IT security life cycle:

- **Phase 1: Initiation**—the organization determines if it should investigate whether implementing an IT security service might improve the effectiveness of the organization's IT security program.
- **Phase 2: Assessment**—the organization determines the security posture of the current environment using metrics and identifies the requirements and viable solutions.
- **Phase 3: Solution**—decision makers evaluate potential solutions, develop the business case, and specify the attributes of an acceptable service arrangement solution from the set of available options.
- **Phase 4: Implementation**—the organization selects and engages the service provider, develops a service arrangement, and implements the solution.
- **Phase 5: Operations**—the organization ensures operational success by consistently monitoring service provider and organizational security performance against identified requirements, periodically evaluating changes in risks and threats to the organization and ensuring the organizational security solution is adjusted as necessary to maintain an acceptable security posture.
- **Phase 6: Closeout**—the organization ensures a smooth transition as the service ends or is discontinued.

Security Services: Issues and Types

The factors to be considered when selecting, implementing, and managing IT security services include the type of service arrangement; service provider qualifications, operational requirements and capabilities, experience, and viability; trustworthiness of service provider employees; and the service provider's capability to deliver adequate protection for the organization systems, applications, and information. These considerations will apply to some degree to every service depending on the size, type, complexity, cost, and criticality of the services being considered and the specific needs of the organization implementing or contracting for the services.

An effective security program has many layers of protection. Using risk management procedures, organizations should evaluate the value of their systems and their information, and then select the security controls that are appropriate for the determined levels of risk. Security programs at both the organizational and system levels should include an appropriate mix of management, operational, and technical controls. Technical controls alone are not sufficient for robust security.

Security services can be obtained to assist organizations in addressing these management, operational, and technical issues:

- **Management Services:** Techniques and concerns normally addressed by management in the organization's information security program, including managing risks. These

services help organizations develop and maintain their security programs, effectively implement and evaluate their programs, develop security architectures, and evaluate IT security products.

- **Operational Services:** Services focused on controls implemented and executed by people, often requiring technical or specialized expertise and relying on management activities and technical controls. These services include assistance with contingency planning, the establishment of incident handling processes, the testing of security controls, and conducting security training.
- **Technical Services:** Services focused on the security controls that a system executes, and dependent on the proper function of the system for effectiveness. These services include firewall installation and maintenance, intrusion detection systems, and the design and development of a Public Key Infrastructure (PKI) system.

While not every available security service is discussed in the guide, the issues and considerations related to the services life cycle are presented. These issues and considerations should be useful in meeting current needs and in addressing future needs as technology changes.

NIST Recommendations

NIST recommends that organizations planning to acquire IT security services should:

- Develop careful, objective business cases. The need for an IT security service should be supported by the business needs of the organization. A business case containing an analysis of the proposed solution, cost estimate, benefits analysis, project risk analysis, and an evaluation of other considered alternatives should provide sufficient documentation to describe and support these needs.
- Develop strong, specific service agreements that define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instances of noncompliance.
- Use metrics throughout the IT security life cycle. Metrics will provide the objective data to evaluate the baseline level of service in the assessment phase and assess service provider performance in the operations phase. Wherever possible, metrics should be selected to indicate progress toward the achievement or maintenance of a security condition that meets an underlying organizational need.
- Develop processes and procedures that can effectively track the myriad service agreements and the metrics that will be applied throughout the life cycle of the many different and disparate IT security services within an organization.
- Ensure that an appropriate transition (bedding in) period is in place between an existing service provider or capability and the new service provider.
- Maintain the technical expertise necessary to understand and manage the security service being provided and to protect the data critical to an organization's mission.

Pay careful attention to six issue areas: strategy/mission, budget/funding, technology/architecture, organization, personnel, and policy/process.

More Information

Federal organizations should consult OMB Circular A-76, *Performance of Commercial Activities*, for information on establishing the foundation for decisions concerning whether activities should be performed under contract with a commercial activity or performed in-house using government facilities and personnel.

For a complete list of references to publications and web pages with information that can help you in selecting, implementing, and managing IT security services, consult Appendix A of NIST SP 800-35.

NIST Special Publications, including the following, are available in electronic format from the Computer Security Resource Center at http://csrc.nist.gov/publications.

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

NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, explains a framework for IT security training requirements and emphasizes results-based learning.

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

NIST SP 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, discusses the concept of assurance in the acquisition and use of security products.

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.

NIST SP 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, assists federal agencies in using PKI for digital signatures and authentication over open networks.

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 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, advises federal organizations on how to determine if a PKI is appropriate for them and how to use PKI services effectively.

NIST SP 800-33, *Underlying Technical Models for Information Technology Security*, provides information on IT security engineering principles and concepts for IT systems.

NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, guides organizations in preparing and maintaining IT contingency plans.

NIST SP 800-36, *Guide to Selecting Information Technology Security Products*, helps organizations select cost-effective and useful products for their IT systems.

NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, describes the fundamental concepts of the certification and accreditation processes, and details the various tasks in the processes.

NIST SP 800-42, *Guideline 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 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*, discusses wireless security issues for local area networks, personal area networks, and handheld devices.

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, provides guidelines to help federal organizations meet their security training responsibilities and build a comprehensive awareness and training program.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, provides information about selecting security controls to meet the security requirements for the system (available in draft at http://csrc.nist.gov/publications/drafts.html).

NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*, helps organizations understand the importance of using metrics and developing a metrics program.

NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*, discusses the analysis of system security requirements and methods for incorporating security into IT procurements.

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