April 1999

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

GUIDE FOR DEVELOPING SECURITY PLANS FOR INFORMATION TECHNOLOGY SYSTEMS

Today's rapidly changing technical environment requires federal agencies to adopt a minimum set of management controls to protect vital information technology (IT) resources. These management controls are directed at individual IT users in order to reflect the distributed nature of today's technology. Technical and operational controls support management controls. To be effective, all of these controls must interrelate.

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology recently published Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*. Developed by Marianne Swanson and a working group of the Federal Computer Security Program Managers' Forum, the publication addresses the development of security plans that document the management, technical, and operational controls for federal automated information systems. The publication provides guidance for individuals responsible for IT security at the system level and at the organization level. It is written specifically for individuals with little or no computer security expertise. The document can also be used as an auditing tool by auditors, managers, and IT security officers. The concepts presented are generic and can be applied to organizations in private and public sectors. This *ITL Bulletin* summarizes the purpose, responsibilities, format, and development of an effective security plan (the guide provides detailed information).

Background

The completion of system security plans is a requirement of the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," updated in 1996, and of Public Law 100-235, "Computer Security Act of 1987." OMB Circular A-130, Appendix III, does not distinguish between sensitive and non-sensitive systems. Rather, consistent with the Computer Security Act of 1987, the Circular recognizes that federal automated information systems have varied sensitivity and criticality. All federal systems have some level of sensitivity and require protection as part of good management practice. OMB Bulletin 90-08, dated July 9, 1990, which provided initial security planning guidance, is superseded by the issuance of Special Publication 800-18. The generic term "system" is used in the document to mean either a *major application* or a *general support system*.

Major Application or General Support System Plans

All applications and systems must be covered by system security plans if they are categorized as a "major application" or "general support system." Specific security plans for other applications are not required because the security controls for those applications or systems would be provided by the general support systems in which they operate. For example, a department-wide Financial Management System would be a major application requiring its own security plan. A local program

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 address to this office.

Bulletins issued since November 1997:

designed to track expenditures against an office budget might not be considered a major application and would be covered by a general support system security plan for an office automation system or a local area network (LAN). Standard commercial off-the-shelf software (such as word processing software, electronic mail software, utility software, or other general-purpose software) would not typically be considered a major application and would be covered by the plans for the general support system on which they are installed.

Purposes of System Security Plans

- Provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements; and
- Delineate responsibilities and expected behavior of all individuals who access the system.

Security Plan Responsibilities

The system owner is responsible for ensuring that the security plan is prepared and for implementing the plan and monitoring its effectiveness. Security plans should reflect input from various individuals with responsibilities concerning the system, including functional "end users," information owners, the system administrator, and the system security manager.

Agencies may require contractor compliance with the guide as a contract requirement. A security plan in the format specified in the document or in another agreed-upon format is suggested in those cases where vendors are operating a system under contract to the federal government. In those instances where a contractor or other entity (e.g., state or local government) operates a system that supports a federal function, a security plan is required.

OMB Circular A-130 requires a summary of the security plan to be incorporated into the strategic IRM plan required by the Paperwork Reduction Act (44 U.S.C. Chapter 35).

Agencies should develop policy on the security planning process. Security plans are living documents that require periodic reviews, modifications, and milestone or completion dates for planned controls. Procedures should be in place outlining who reviews the plans and follows up on planned controls. In addition, procedures are needed describing how security plans will be used in the authorization for processing process.

Recommended Format

While the format in Special Publication 800-18 is recommended, it is recognized that some agencies have developed plans using other formats that meet A-130 requirements. The document is intended as guidance only and should not be construed as the only format allowed. A standardized approach, however, not only makes the development of the plan easier by providing examples, but also provides a baseline to review plans. The level of detail included within the plan should be consistent with the criticality and value of the system to the organization's mission (i.e., a more detailed plan is required for systems critical to the organization's mission). The security plan should fully identify and describe the controls currently in place or planned for the system and should include a list of *rules of behavior* (see Appendices A and B of the document).

System Analysis

Once completed, a security plan will contain technical information about the system, its security requirements, and the controls implemented to provide protection against its *risks* and vulnerabilities. Before the plan can be developed, a determination must be made as to which type of plan is required for a system. An analysis of the system determines the boundaries of the system and the type of system.

System Boundaries

Defining what constitutes a "system" for the purposes of the guideline requires an analysis of system boundaries and organizational responsibilities. Constructing logical boundaries around a set of processes, communications, storage, and related resources, as defined by the guideline, identifies a system. The elements within these boundaries constitute a single system requiring a security plan. Each element of the system must:

- Be under the *same* direct management control;
- Have the *same* function or mission objective;
- Have essentially the *same* operating characteristics and security needs; and
- Reside in the *same* general operating environment.

All components of a system need not be physically connected (e.g., a group of stand-alone personal computers (PCs) in an office; a group of PCs placed in employees' homes under defined telecommuting pro-

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.

gram rules; a group of portable PCs provided to employees who require mobile computing capability for their jobs; and a system with multiple identical configurations that are installed in locations with the same environmental and physical safeguards).

Multiple Similar Systems

An organization may have systems that differ only in the responsible organization or the physical environment in which they are located (e.g., air traffic control systems). In such instances, it is appropriate and recommended to use plans that are identical except for those areas of difference. This approach provides consistent levels of protection for similar systems.

System Category

The next step is to categorize each system as either a "*major application*" or as a "*general support system*." All applications should be covered by a security plan. The applications will either be covered individually if they have been designated as a major application or within the security plan of a general support system. A system may be designated as a major application even though it is also supported by a system that has been designated as a general support system. For example, a LAN may be designated a general support system and have a security plan. The organization's accounting system may be designated as a major application even though the computing and communication resources of the LAN support it. In this example, the major application requires additional security requirements due to the sensitivity of the information the application processes. When a security plan is required for a major application that is supported by a general support system, coordination of both plans is required.

■ *Major Applications*

All federal applications have value and require some level of protection. Certain applications, because of the information they contain, process, or transmit or because of their criticality to the organization's missions, require special management oversight. These applications are major applications.

Agencies are expected to exercise management judgment in determining which of their applications is a major application and to ensure that the security requirements of non-major applications are discussed as part of the security plan for the applicable general support systems.

Major applications are systems that perform clearly defined functions for which there are readily identifiable security considerations and needs (e.g., an electronic funds transfer system). A major application might comprise many individual programs and hardware, software, and telecommunications components. These components can be a single software application or a combination of hardware/software focused on supporting a specific mission-related function. A major application may also consist of multiple individual applications if all are related to a single mission function (e.g., payroll or personnel). If a system is defined as a major application and the application is run on another organization's general support system:

- ❒ Notify the system owner that the application is critical or contains *sensitive information* and provide specific security requirements;
- ❒ Provide a copy of the major application's security plan to the operator of the general support system;
- ❒ Request a copy of the system security plan of the general support system and ensure it provides adequate protection for the application and information; and
- ❒ Include a reference to the general support system security plan, including the unique name/identifier information.

■ *General Support System*

A general support system is interconnected information resources under the same direct management control that shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. A general support system, for example, can be a:

- ❒ LAN including smart terminals that supports a branch office;
- ❒ Backbone (e.g., agency-wide);
- ❒ Communications network;
- ❒ Departmental data processing center including its operating system and utilities;
- ❒ Tactical radio network; or
- ❒ Shared information processing service organization.

A major application can run on a general support system. The general support system plan should reference the major application plan(s).

Plan Development for All Systems

All security plans, at a minimum, should be marked, handled, and controlled to the level of sensitivity determined by organizational policy.

In addition, all security plans should be dated for ease of tracking modifications and approvals. Dating each page of a security plan may be appropriate if updates are to be made through change pages. Both types of plans must contain general descriptive information regarding who is responsible for the system, the purpose of the system, and the *sensitivity* level of the system.

System Identification

- *System Name/Title*
  The plan begins with listing the name and title of the system/application. Each system/application should be assigned a unique name/identifier. Assigning a unique identifier to each system helps to ensure that appropriate security requirements are met based on the unique requirements for the system, and that allocated resources are appropriately applied. Further, the use of unique system identifiers is integral to the IT system investment models and analyses established under the requirements of the Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act). The identifier could be a combination of alphabetic and numeric characters and can be used in combination with the system/application name. The unique name/identifier should remain the same throughout the life of the system to allow the organization to track completion of security requirements over time.
- *Responsible Organization*
  List the federal organizational subcomponent responsible for the system. If a state or local government or contractor performs the function, identify both the federal and other organization and describe the relationship. Be specific about the organization and do not abbreviate. Include physical locations and addresses.
- *Information Contact(s)*
  List the name, title, organization, and telephone number of one or more persons designated to be the point(s) of contact for this system. One of the contacts given should be identified as the system owner. The designated persons should have sufficient knowledge of the system to be able to provide additional information or points of contact, as needed.
- *Assignment of Security Responsibility*
  An individual must be assigned responsibility in writing to ensure that the application or general support system has adequate security. To be effective, this individual must be knowledgeable of the management, operational, and technical controls used to protect the system. Include the name, title, and telephone number of the individual who has been assigned responsibility for the security of the system.

System Operational Status

Indicate one or more of the following for the system's operational status. If more than one status is selected, list which part of the system is covered under each status.

- *Operational* — the system is operating.
- *Under development* — the system is being designed, developed, or implemented.
- *Undergoing a major modification* — the system is undergoing a major conversion or transition.

If the system is under development or undergoing a major modification, provide information about the methods used to assure that up-front security requirements are included. Include specific controls in the appropriate sections of the plan depending on where the system is in the security life cycle.

General Description/ Purpose

Present a brief description (one-three paragraphs) of the function and purpose of the system (e.g., economic indicator, network support for an organization, business census data analysis, crop-reporting support).

If the system is a general support system, list all applications supported by the general support system. Specify if the application is or is not a major application and include unique name/identifiers, where applicable. Describe each application's function and the information processed. Include a list of user organizations, whether they are internal or external to the system owner's organization, and a general description of the type of information and processing provided. Request information from the application owners (and a copy of the security plans for major applications) to ensure their requirements are met.

System Environment

Provide a brief (one-three paragraphs) general description of the technical system. Include any environmental or technical factors that raise special security concerns, such as:

- The system is connected to the Internet;
- It is located in a harsh or overseas environment;
- Software is rapidly implemented;
- The software resides on an open network used by the general public or with overseas access;

- The application is processed at a facility outside of the organization's control; or

- The general support mainframe has dial-up lines.

Describe the primary computing platform(s) used (e.g., mainframe, desk top, LAN or Wide Area Network (WAN). Include a general description of the principal system components, including hardware, software, and communications resources. Discuss the type of communications included (e.g., dedicated circuits, dial circuits, public data/voice networks, Internet). Describe controls used to protect communication lines in the appropriate sections of the security plan.

Include any security software protecting the system and information. Describe in general terms the type of security protection provided (e.g., access control to the computing platform and stored files at the operating system level or access to data records within an application). Include only controls that have been implemented or are planned, rather than listing the controls that are available in the software. Controls that are available, but not implemented, provide no protection.

System Interconnection/ Information Sharing

System interconnection is the direct connection of systems for the purpose of sharing information resources. System interconnection, if not appropriately protected, may result in a compromise of all connected systems and the data they store, process, or transmit. It is important that system operators, information owners, and management obtain as much information as possible about the vulnerabilities associated with system interconnection and information sharing and the increased controls required to mitigate those vulnerabilities. The security plan for the systems often serves as a mechanism to effect this security information exchange and allows management to make informed decisions regarding risk reduction and acceptance.

OMB Circular A-130 requires that written management authorization (often in the form of a Memorandum of Understanding or Agreement) be obtained prior to connecting with other systems and/or sharing sensitive data/information. The written authorization shall detail the rules of behavior and controls that must be maintained by the interconnecting systems. A description of the rules for interconnecting systems and for protecting shared data must be included with this security plan.

In this section, provide the following information concerning the authorization for the connection to other systems or the sharing of information:

- List of interconnected systems (including Internet);

- Unique system identifiers, if appropriate;

- Name of system(s);

- Organization owning the other system(s);

- Type of interconnection (TCP/IP, Dial, SNA, etc.);

- Short discussion of major concerns or considerations in determining interconnection;

- Name and title of authorizing management official(s);

- Date of authorization;

- System of Record, if applicable (Privacy Act data);

- Sensitivity level of each system;

- Interaction among systems; and

- Security concerns and Rules of Behavior (see Appendices A and B of the guide) of the other systems that need to be considered in the protection of this system.

Sensitivity of Information Handled

This section provides a description of the types of information handled by the system and an analysis of the criticality of the information. The sensitivity and criticality of the information stored within, processed by, or transmitted by a system provides a basis for the value of the system and is one of the major factors in *risk management*. The description will provide information to a variety of users, including:

- Analysts/programmers who will use it to help design appropriate security controls;

- Internal and external auditors evaluating system security measures; and

- Managers making decisions about the reasonableness of security countermeasures.

The nature of the information sensitivity and criticality must be described in this section. The description must contain information on applicable laws, regulations,

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 to listproc@nist.gov with the message **subscribe itl-bulletin**, and your proper 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.

and policies affecting the system and a general description of sensitivity.

The remainder of the guidance document details the management, operational, and technical controls, discussed for both major applications and general support systems. Appendices include Rules of Behavior, templates for security plans, a glossary, references, and an index.

For more information

The planning guideline is available at http://csrc.nist.gov/nistpubs/ for download in Microsoft Word '97 (.doc) and Adobe Acrobat (.pdf) formats. Paper copies can be ordered from the Government Printing Office at (202) 512-1800; the order number is SN003-003-03590-4 and the price is $14.00. Paper copies are also available from the National Technical Information Service (NTIS) at (703) 605-6000; order number is PB99-105116.

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

BULK RATE
POSTAGE & FEES
PAID
NIST
PERMIT NUMBER G195