September 2001

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

SECURITY SELF-ASSESSMENT GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS

Marianne Swanson, Author,
Elizabeth B. Lennon, Editor
Information Technology Laboratory,
National Institute of Standards and Technology

Introduction

Adequate security of information and the systems that process it is a fundamental management responsibility. Federal agencies must plan for security, ensure that the appropriate officials are assigned security responsibility, and authorize system processing prior to operations and periodically thereafter. These management responsibilities presume that responsible agency officials understand the risks and other factors that could negatively impact their mission goals. Moreover, these officials must understand the current status of security programs and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

One method used to measure information technology (IT) security assurance is a self-assessment conducted on a system (major application or general support system) or multiple self-assessments conducted for a group of interconnected systems (internal or external to the agency). Self-assessments provide a cost-effective technique for agency officials to determine the current status of their information security programs, mitigate identified weaknesses, and where necessary, establish a target for improvement.

Guidance on the Self-Assessment Process

ITL has issued a new guidance document on the self-assessment process. NIST Special Publication (SP) 800-26, *Security Self-Assessment Guide for Information Technology Systems,* utilizes an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured. This *ITL Bulletin* summarizes the new document, available in two formats from http://csrc.nist.gov/publications/nistpubs/index.html. While this guidance document applies primarily to federal agencies, private sector organizations may also find the self-assessment approach a valuable tool.

The guide does not establish new security requirements. The control objectives and techniques are abstracted directly from long-standing requirements found in statute, policy, and guidance on security. The document builds on the *Federal IT Security Assessment Framework* (Framework) developed by NIST for the Federal Chief Information Officer (CIO) Council. The Framework established the groundwork for standardizing on five levels of security status and criteria agencies could use to determine if the five levels were adequately implemented. The new document provides guidance on applying the Framework by identifying 17 control areas, such as those pertaining to identification and authentication and contingency planning. In addition, the guide provides control objectives and techniques that can be measured for each area.

Finally, the document provides guidance on utilizing the results of the system self-assessment to ascertain the status of the agency-wide security program. The results are obtained in a form that can readily be used to determine which of the five levels specified in the Framework the agency has achieved for each topic area covered in the questionnaire. For example, the group of systems under review may have reached level 4 (Tested and Evaluated Procedures and Controls) in the topic area of physical and environmental protection, but only level 3 (Implemented Procedures and Controls) in the area of logical access controls.

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 March 2000

Audience

The control objectives and techniques presented are generic and can be applied to organizations in private and public sectors. The document can be used by all levels of management and by those individuals responsible for IT security at the system level and organization level. Additionally, internal and external auditors may use the questionnaire to guide their review of the IT security of systems. To perform the examination and testing required to complete the questionnaire, the assessor must be familiar with and able to apply a core knowledge set of IT security basics needed to protect information and systems. In some cases, especially in the area of examining and testing technical controls, assessors with specialized technical expertise will be needed to ensure that the questionnaire's answers are reliable.

Uses of the Self-Assessment Questionnaire

The questionnaire can be used for the following purposes:

- Agency managers who know their agency's systems and security controls can quickly gain a general understanding of needed security improvements for a system (major application or general support system), group of interconnected systems, or the entire agency.
- The security of an agency's system can be thoroughly evaluated using the questionnaire as a guide. The results of such a thorough review produce a reliable measure of security effectiveness and may be used to fulfill reporting requirements, prepare for audits, and identify resources.
- The results of the questionnaire will assist, but not fulfill, agency budget requests as outlined in Office of Management and Budget (OMB) Circular A-11, "Preparing and Submitting Budget Estimates."

It is important to note that the questionnaire is not intended to be an all-inclusive list of control objectives and related techniques. Accordingly, it should be used in conjunction with the more detailed guidance listed in Appendix B of the document. In addition, details associated with certain technical controls are not specifically provided due to their voluminous and dynamic nature. Agency managers should obtain information on such controls from other sources, such as vendors, and use that information to supplement this guide.

> For a self-assessment to be effective, a risk assessment should be conducted in conjunction with or prior to the self-assessment.

System Analysis

Before the questionnaire can be used effectively, a determination must be made as to the boundaries of the system and the sensitivity and criticality of the information stored within, processed by, or transmitted by the system(s). The security of every system or group of interconnected system(s) must be described in a security plan. If a plan has not been prepared for the system, the completion of the self-assessment will aid in developing the system security plan. Many of the control objectives addressed in the assessment are to be described in the system security plan.

Defining the scope of the assessment requires an analysis of system boundaries and organizational responsibilities. As defined in NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, a system is identified by defining boundaries around a set of processes, communications, storage, and related resources. 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. See http://csrc.nist.gov/publications/nistpubs/index.html for additional guidance from NIST SP 800-18.

Effective use of the questionnaire presumes a comprehensive understanding of the value of the systems and information being assessed. Value can be expressed in terms of the degree of sensitivity or criticality of the systems and information relative to the three basic protection categories of confidentiality, integrity, and availability. In addition, it is helpful to categorize the system or group of systems by sensitivity level, i.e., high, medium, or low.

Questionnaire Structure

The self-assessment questionnaire contains three sections: cover sheet, questions, and notes. The questionnaire begins with a cover sheet requiring descriptive information about the major application, general support system, or group of interconnected systems being assessed. The questionnaire provides a hierarchical approach to assessing a system by containing critical elements and subordinate questions. Assessors will need to carefully review the levels of subordinate control objectives and techniques in order to determine what level has been reached for the related critical element. The questionnaire section may be customized by the organization. An organization can add questions, require more descriptive information, and even pre-mark certain questions if applicable. The notes section can be used to document findings and to indicate follow-up actions. The time required to complete an evaluation will vary, as will the needed resources.

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 web site is http://www.itl.nist.gov/.

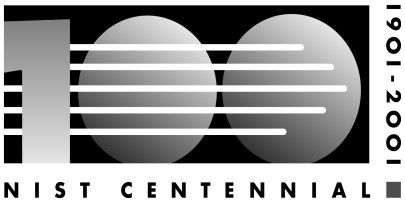
Conclusion

Consistent with OMB policy, each agency must implement and maintain a program to adequately secure its information and system assets. An agency program must: 1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability; and 2) protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification. Performing a self-assessment and mitigating any of the weaknesses found in the assessment is one way to determine if the system and the information are adequately secured.

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.

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