May 2004

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

GUIDE FOR THE SECURITY CERTIFICATION AND ACCREDITATION OF FEDERAL INFORMATION SYSTEMS

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

Introduction

In response to the requirements of the E-Government Act (Public Law 107-347), Title III, Federal Information Security Management Act (FISMA) of December 2002, ITL recently published NIST Special Publication (SP) 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*. Developed through an extensive public review process, the document represents a significant contribution to federal agency security management by providing specific recommendations on how to certify and accredit information systems. State, local, and tribal governments, as well as private sector organizations, are encouraged to use the guidelines, as appropriate. This *ITL Bulletin* summarizes the document, which is available at http://csrc.nist.gov/sec-cert/.

NIST SP 800-37 provides guidelines for the security certification and accreditation of information systems supporting the executive agencies of the federal government. The guidelines have been developed to help achieve more secure information systems within the federal government by:

- Enabling more consistent, comparable, and repeatable assessments of security controls in federal information systems;
- Promoting a better understanding of agency-related mission risks resulting from the operation of information systems; and
- Creating more complete, reliable, and trustworthy information for authorizing officials—to facilitate more informed security accreditation decisions.

Security Certification and Accreditation

Security certification and accreditation are important activities that support a risk management process and an integral part of an agency's information security program.

Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. Required by OMB Circular A-130, Appendix III, security accreditation provides a form of quality control and challenges managers and technical staffs at all levels to implement the most effective security controls possible in an information system, given mission requirements, technical constraints, operational constraints, and cost/schedule constraints. By accrediting an information system, an agency official accepts responsibility for the security of the system and is fully *accountable* for any adverse impacts to the agency if a breach of security occurs. Thus, responsibility and accountability are core principles that characterize security accreditation.

It is essential that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems. The information and supporting evidence needed for security accreditation is often developed during a detailed security review of an information system, typically referred to as security *certification*. Security certification is a comprehensive assessment of the management, operational, and technical security controls in an

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 January 2002

information system, made in support of security accreditation, 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. The results of a security certification are used to reassess the risks and update the system security plan, thus providing the factual basis for an authorizing official to render a security accreditation decision.

Roles and Responsibilities

NIST SP 800-37 describes the roles and responsibilities of key participants, summarized below, involved in an agency's security certification and accreditation process:

- The *Chief Information Officer* is the agency official responsible for: (i) designating a senior agency information security officer; (ii) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements; (iii) training and overseeing personnel with significant responsibilities for information security; (iv) assisting senior agency officials concerning their security responsibilities; and (v) in coordination with other senior agency officials, reporting annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

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/.

- The *authorizing official* (or designated approving/accrediting authority as referred to by some agencies) is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals.
- The authorizing official's *designated representative* is an individual acting on the authorizing official's behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of an information system.
- The *senior agency information security officer* is the agency official responsible for: (i) carrying out the Chief Information Officer responsibilities under FISMA; (ii) possessing professional qualifications, including training and experience, required to administer the information security program functions; (iii) having information security duties as that official's primary duty; and (iv) heading an office with the mission and resources to assist in ensuring agency compliance with FISMA.
- The *information system owner* is an agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
- The *information owner* is an agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
- The *information system security officer* is the individual responsible to the authorizing official, information system owner, or the senior agency information security officer for ensuring the appropriate operational security posture is maintained for an information system or program.
- The *certification agent* is an individual, group, or organization responsible for conducting a security certification, or comprehensive assessment of the management, operational, and technical security controls in an information system 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.
- *User representatives* are individuals that represent the operational interests of the user community and serve as liaisons for that community throughout the system development life cycle of the information system.

At the discretion of senior agency officials, certain security certification and accreditation roles may be delegated, and if so, appropriately documented. Individuals serving in delegated roles are able to operate with the authority of agency officials within the limits defined for the specific certification and accreditation activities. Agency officials retain ultimate responsibility, however, for the results of actions performed by individuals serving in delegated roles.

The Process

The security certification and accreditation process consists of four distinct phases:

- Initiation Phase;
- Security Certification Phase;
- Security Accreditation Phase; and
- Continuous Monitoring Phase.

Each phase in the security certification and accreditation process consists of a set of well-defined tasks and subtasks that are to be carried out, as indicated, by responsible individuals (e.g., the Chief Information Officer, authorizing official, authorizing official's designated representative, senior agency information security officer, information system owner, information owner, information system security officer, certification agent, and user representatives).

The *Initiation Phase* consists of three tasks: (i) preparation; (ii) notification and resource identification; and (iii) system security plan review, analysis, and acceptance. The purpose of this phase is to ensure that the authorizing

official and senior agency information security officer are in agreement with the contents of the system security plan before the certification agent begins the assessment of the security controls in the information system.

The *Security Certification Phase* consists of two tasks: (i) security control assessment; and (ii) security certification documentation. The purpose of this phase is to determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. This phase also addresses specific actions taken or planned to correct deficiencies in the security controls and to reduce or eliminate known vulnerabilities in the information system. Upon successful completion of this phase, the authorizing official will have the information needed from the security certification to determine the risk to agency operations, agency assets, or individuals, and thus will be able to render an appropriate security accreditation decision for the information system.

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 Accreditation Phase* consists of two tasks: (i) security accreditation decision; and (ii) security accreditation documentation. The purpose of this phase is to determine if the remaining known vulnerabilities in the information system (after the implementation of an agreed-upon set of security controls) pose an acceptable level of risk to agency operations, agency assets, or individuals. Upon successful completion of this phase, the information system owner will have: (i) authorization to operate the information system; (ii) an interim authorization to operate the information system under specific terms and conditions; or (iii) denial of authorization to operate the information system.

The *Continuous Monitoring Phase* consists of three tasks: (i) configuration management and control; (ii) security control monitoring; and (iii) status reporting and documentation. The purpose of this phase is to provide oversight and monitoring of the security controls in the information system on an ongoing basis and to inform the authorizing official when changes occur that may impact on the security of the system. The activities in this phase are performed continuously throughout the life cycle of the information system.

Accreditation Decisions

The security *accreditation package* documents the results of the security certification and provides the authorizing official with the essential information needed to make a credible, risk-based decision on whether to authorize operation of the information system. Security accreditation decisions resulting from security certification and accreditation processes should be conveyed to information system owners. To ensure the agency's business and operational needs are fully considered, the authorizing official should meet with the information system owner prior to issuing the security accreditation decision to discuss the security certification findings and the terms and conditions of the authorization. There are three types of accreditation decisions that can be rendered by authorizing officials:

- Authorization to operate;
- Interim authorization to operate; or
- Denial of authorization to operate.

Examples of security accreditation decision letters appear in Appendix E.

Continuous Monitoring

A critical aspect of the security certification and accreditation process is the post-accreditation period involving the continuous monitoring of security controls in the information system over time. An effective continuous monitoring program requires:

- Configuration management and configuration control processes;
- Security impact analyses on changes to the information system; and
- Assessment of selected security controls in the information system and security status reporting to appropriate agency officials.

Conclusion

Completing a security accreditation ensures that an information system will be operated with appropriate management review, that there is ongoing monitoring of security controls, and that re-accreditation occurs periodically in accordance with federal or agency policy and whenever there is a significant change to the system or its operational environment.

***Disclaimer**: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology 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