NIST Special Publication 800-37

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Guide for the Security Certification and Accreditation of Federal Information Systems

Ron Ross and Marianne Swanson

I N F O R M A T I O N S E C U R I T Y

SECOND PUBLIC DRAFT

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

June 2003

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of non-national security-related information in federal information systems. This special publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov — Phone: (202) 512-1800 — Fax: (202) 512-2250
Mail: Stop SSOP, Washington, DC 20402-0001

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

National Institute of Standards and Technology Special Publication 800-37, 62 pages (June 2003) CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

THE PUBLIC COMMENT PERIOD FOR THIS DOCUMENT BEGINS ON JULY 1, 2003 AND ENDS ON 31 AUGUST 2003. COMMENTS MAY BE SUBMITTED TO THE COMPUTER SECURITY DIVISION, NIST, VIA ELECTRONIC MAIL AT SEC-CERT@NIST.GOV

OR VIA REGULAR MAIL AT

100 BUREAU DRIVE (MAIL STOP 8930)
GAITHERSBURG, MD 20899-8930

Acknowledgements

The authors, Ron Ross and Marianne Swanson of the National Institute of Standards and Technology (NIST) wish to thank their colleagues who reviewed drafts of this document and contributed to its development. The authors also gratefully acknowledge and appreciate the many comments from the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

Note to Reviewers

Reviewers of NIST Special Publication 800-37 will notice important and significant changes in this current release of the document. Recent legislation promulgated in the Federal Information Security Management Act (FISMA) of 2002 and the feedback from the public and private sectors during the initial comment period have prompted these changes. Special Publication 800-37 has been reengineered to better support the information security programs in federal agencies. The security certification and accreditation guidelines will be used in conjunction with an emerging family of security-related publications including:

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, (Initial public draft), May 2003;
- NIST Special Publication 800-53, *Security Controls for Federal Information Systems*, (Initial public draft projected for publication, Summer 2003);
- NIST Special Publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems*, (Initial public draft projected for publication, Winter 2003-04);
- NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Objectives and Risk Levels*, (Initial public draft projected for publication, Fall 2003).

The series of five documents, when completed, is intended to provide a structured, yet flexible framework for identifying, employing, and evaluating the security controls in federal information systems—and thus, satisfy the requirements of the FISMA legislation. We regret that all five publications could not be released simultaneously. However, due to the current international climate and high priority of information security for our federal agencies, we have decided to release the individual publications as they are completed. While the publications are mutually reinforcing and have some dependencies, in most cases, they can be effectively used independently of one another. None of the special publications will be published in final form until all of the documents have completed an extensive public review process and have been finalized.

The following substantive changes have been made to Special Publication 800-37—

- Clarification and redefinition of authorizing official, information system owner, and certification agent roles and responsibilities;
- Identification of a new role in the security certification and accreditation process—that of authorizing official's designated representative;
- Differentiation between the concepts of information system vulnerabilities and residual risk to agency operations or assets;
- Elimination of security certification levels;
- Redesign of the security certification and accreditation process to include new initiation and continuous monitoring phases and associated tasks and subtasks; and
- Incorporation of draft FIPS Publication 199 security categorization standards and risk levels into the security certification and accreditation process.

Your continued feedback during the public comment periods is essential to the document development process and is greatly appreciated.

-- Ron Ross and Marianne Swanson

Table of Contents

List of Figures

CHAPTER ONE **1**

INTRODUCTION

THE NEED FOR SECURITY CERTIFICATION AND ACCREDITATION

"Confidence in information systems security can be gained through actions taken during the processes of development, evaluation, and operation."

The E-Government Act (Public Law 107-347) passed by the one hundred and seventh Congress and signed into law by the President in December 2002 recognized the importance of information security[1] to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), requires each federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems[2] that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The information security program must include—

- Periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system;
- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the agency) of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls[3] to be performed with a frequency depending on risk, but no less than annually;
- A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices, of the agency;
- Procedures for detecting, reporting, and responding to security incidents; and
- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

[1] Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

[2] An information system is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[3] Security controls are the management, operational, and technical controls (i.e., safeguards or countermeasures), prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information.

FISMA, along with the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), explicitly emphasizes a risk-based policy for cost-effective security. In support of and reinforcing this legislation, the Office of Management and Budget (OMB) through Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, requires executive agencies[4] within the federal government to: (i) plan for security; (ii) ensure that appropriate officials are assigned security responsibility; (iii) periodically review the security controls in their information systems; and (iv) 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 adversely affect their missions. Moreover, these officials must understand the current status of their security programs and the security controls planned or in place to protect their information and information systems in order to make informed judgments and investments that appropriately mitigate risk to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the agency and to accomplish the agency's stated missions with what OMB Circular A-130 defines as *adequate security*, or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

Security accreditation is the official management decision to authorize operation of an information system. This authorization, given by a senior agency official, is applicable to a particular environment of operation, and explicitly accepts the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, remaining after the implementation of an agreed upon set of security controls. By accrediting an information system, the agency official is not only responsible for the security of the system but is also accountable for adverse impacts to the agency if a breach of security occurs. Security accreditation, which is required under OMB Circular A-130, provides a form of quality control and challenges managers and technical staff at all levels to implement the most effective security controls and techniques, given technical constraints, operational constraints, cost and schedule constraints, and mission requirements.

The assessment of risk and the development of security plans are two important activities in an agency's information security program that directly support the security accreditation process and are required under FISMA and OMB Circular A-130. Risk assessments,[5] whether done formally or informally, influence the development of the security requirements and the security controls for information systems and generate much of the information needed for the associated security plans for those systems. Security plans[6] document the security requirements and security controls for information systems and provide essential information for security accreditations. Security plans typically include as references or attachments, other important security-related documents (e.g., contingency plans, configuration management plans, risk assessments, information system interconnection agreements) that are produced as part of an agency information security program.

[4] An executive agency is: (i) an Executive Department specified in 5 U.S.C., Section 101; (ii) a Military Department specified in 5 U.S.C., Section 102; (iii) an independent establishment as defined in 5 U.S.C., Section 104(1); and (iv) a wholly owned government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.

[5] Risk assessments can be accomplished in a variety of ways depending on the specific needs of the agency. Some agencies may choose to assess risk informally. Other agencies may choose to employ a more formal and structured approach. In either case, the assessment of risk is a process that should be incorporated into the system development life cycle and the process should be reasonable for the agency concerned. At a minimum, documentation should be produced that describes the process employed and describes the results obtained. NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, provides recommendations on conducting risk assessments and is appropriate for either situation described above.

[6] NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, provides guidance and recommendations on the format and content of security plans.

In addition to risk assessments and security plans, security evaluation also plays an important role in the security accreditation process. 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 credible, risk-based decisions on whether to authorize operation of those systems. This information and supporting evidence for system authorization is often developed during a detailed security review of the information system, typically referred to as *security certification.* Security certification is the comprehensive evaluation of the management, operational, and technical security controls in an information system. This evaluation, made in support of the security accreditation process, determines the effectiveness of these security controls in a particular environment of operation and the vulnerabilities in the information system after the implementation of such controls.

The results of the security certification are used to reassess the risks and update the security plan for the information system—thus, providing the factual basis for the authorizing official to render the security accreditation decision. By accrediting the information system, the agency official accepts the risk associated with it and the implications on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Formalization of the security accreditation process ensures that information systems will be operated with appropriate management review, that there is ongoing monitoring of security controls, and that reaccreditation occurs periodically and whenever there is a significant change to the system or its environment.[7] Security certification and accreditation of agency information systems support the legislative requirements of FISMA by ensuring that agencies periodically: (i) assess the risk resulting from the operation of those systems; (ii) test and evaluate the security controls in those systems to determine control effectiveness and system vulnerabilities; and (iii) assess the information security programs supporting those systems (e.g., security awareness and training, incident response, and contingency planning).

1.1 PURPOSE AND APPLICABILITY

The purpose of this special publication is to provide guidelines for certifying and accrediting information systems supporting the executive agencies of the federal government. The security certification and accreditation guidelines have been developed to:

- Enable more consistent, comparable, and repeatable evaluations of security controls applied to federal information systems;[8]
- Promote a better understanding of agency-related risks resulting from the operation of information systems;
- Create more complete, reliable, and trustworthy information for authorizing officials—thus, facilitating more informed security accreditation decisions; and
- Help achieve more secure information systems within the federal government.

The guidelines provided in Special Publication 800-37 are applicable to all federal information systems other than those systems designated as national security systems as defined in 44 U.S.C.,

[7] A significant change to an information system is any change that the responsible agency official believes is likely to affect the confidentiality, integrity, or availability of the system, and thus, adversely impact agency operations (including mission, functions, image or reputation) or agency assets.

[8] A federal information system is an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

Section 3542.[9] The guidelines have been broadly developed from a technical perspective so as to be complementary to similar guidelines issued by agencies and offices operating or exercising control over national security systems. This publication is intended to provide guidelines to federal agencies in lieu of Federal Information Processing Standards (FIPS) Publication 102, *Guidelines for Computer Security Certification and Accreditation*, September 1983, which has been rescinded. State, local, and tribal governments as well as private sector organizations comprising the critical infrastructure of the United States are also encouraged to consider the use of these guidelines, as appropriate.

1.2 SYSTEM DEVELOPMENT LIFE CYCLE

All federal information systems, including operational systems, systems under development, and systems undergoing some form of modification or upgrade, are in some phase of what is commonly referred to as the system development life cycle.[10] There are many activities occurring during the life cycle of an information system dealing with the issues of cost, schedule, and performance. In addition to the functional requirements levied on an information system, security requirements must also be considered. In the end, the information system must be able to meet its functional requirements and do so in a manner that is secure enough to protect the agency's operations (including mission, functions, image, or reputation) and assets. In accordance with the provisions of FISMA, agencies are required to have an information security program and that program should be effectively integrated into the system development life cycle. The security certification and accreditation process is an important part of the agency's information security program, and therefore, the activities associated with certifying and accrediting an information system, should also be integrated into the agency's system development life cycle.

The security certification and accreditation tasks described in this special publication should be appropriately tailored to the life cycle phase of the information system. For systems under development, the security certification and accreditation tasks begin early in the life cycle with an opportunity to shape and influence the security capabilities of the system. For operational systems and many of the older systems in the federal inventory, the security certification and accreditation tasks may, by necessity, begin later in the life cycle. In either situation, all of the certification and accreditation tasks should be completed to ensure that: (i) the information system has received the necessary attention with regard to security; and (ii) the authorizing official explicitly accepts the residual risk to agency operations, agency assets, or individuals after the implementation of an agreed upon set of security controls. Annex F provides additional details on several key information security program activities (including security certification and accreditation) that can be effectively incorporated into the appropriate life cycle phases.

[9] A national security system is any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or, (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

[10] There are typically five phases in the system development life cycle of an information system: (i) initiation; (ii) development and acquisition; (iii) implementation; (iv) operations and maintenance; and (v) disposal.

1.3 COMPONENT PRODUCT EVALUATION PROGRAMS

It is recognized that commercially developed information technology products offer advanced, dynamic, robust, and effective information security solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation. Many federal information systems are procured and constructed to meet specific requirements and typically use existing commercial off-the-shelf information technology component products such as operating systems, database systems, firewalls, network devices, web browsers, smart cards, biometrics devices, general-purpose applications, cryptographic modules, and hardware platforms. In many cases, the security controls implemented within an information system use the security functions of the underlying component products and depend upon the correct operation of those products. Component products may also be subject to security testing and evaluation (for confirming compliance with developer claims) with the results available to support the security certification and accreditation process.[11] Notwithstanding the fact that agencies can rely upon the prior testing and evaluation of the individual components of an information system (provided they are properly installed and configured), there must still be an evaluation of the integrated system and an evaluation in the operational environment to make certain that the proper security functions have been provided and that vulnerabilities have not been introduced during the integration process. Using tested and evaluated component products may significantly reduce the cost of certification and accreditation by facilitating the reuse of test and evaluation results and by providing specific information on how to securely configure particular products within an information system. However, when using previously tested and evaluated component products, care must be taken to ensure that either the configuration of the products will be the same as when they were tested and evaluated or that any differences are accounted for in the system-level security testing and evaluation to follow.

1.4 SECURITY IMPLEMENTATION GUIDANCE

In addition to component product testing and evaluation, guidance on how to securely configure information technology products can be instrumental in helping federal agencies develop, deploy, operate, and maintain more secure information systems. Security implementation guidance provides information and recommendations on appropriate security settings for widely used commercial off-the-shelf information technology products that are being deployed in federal information systems. This implementation guidance is meant to help agencies gain the maximum advantage from the security features provided by the component products—it is not meant, however, to replace well-structured security policy or sound judgment. Furthermore, the security implementation guidance does not address site-specific configuration issues. Care must be taken when employing the implementation guidance to address local operational and policy concerns. Security implementation guidance is available from a variety of federal agencies and several private sector organizations in the form of Security Reference Guides, Security Technical Implementation Guides, checklists, scripts, and other implementation-related recommendations.

[11] Federally sponsored programs for component-level testing and evaluation of general-purpose information technology products and cryptographic modules are available under the National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme and the NIST Cryptographic Module Validation Program, respectively, in accordance with federal and international security standards. Component-level testing and evaluation produces a variety of potentially useful outputs for the security certification and accreditation process, including: (i) certificates attesting to the results of the testing and evaluation; (ii) validation reports; (iii) product security specifications; (iv) proof of compliance to security requirements; (v) evaluation technical reports; and (vi) developer product summaries. Many of the aforementioned documents, along with a listing of evaluated products, are publicly available from the validation authorities responsible for administering these programs. Other documents may be obtainable on a case-by-case basis directly from testing laboratories, product developers, or sponsors of security evaluations.

1.5 OTHER SUPPORTING ASSESSMENT ACTIVITIES

Since the cost of security certification and accreditation can be substantial, it is important to leverage the results of previous assessment-related activities that have been conducted on an agency's information system. For example, assessments of information systems using the NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, the National Security Agency's *INFOSEC Assessment Methodology*, or the General Accounting Office *Federal Information System Controls Audit Manual*, can support the security certification and accreditation process in several ways. First, these assessments can be used to gauge the preparedness of an information system for security certification and accreditation by examining the status of key security controls in the system. Second, the results produced during these assessments can be considered and potentially reused as evidence, when appropriate, during the security certification and accreditation process, specifically during the testing and evaluation of security controls. Bringing in evidence of security control effectiveness from multiple sources (e.g., self-assessments, INFOSEC assessments, audits, security reviews) not only reduces the potential cost of security certification and accreditation but also increases the overall confidence in the final results.

1.6 ORGANIZATION OF THIS SPECIAL PUBLICATION

This special publication contains three main chapters and six supporting annexes. Chapter 1 introduces the concept of security certification and accreditation in the context of FISMA and OMB-related requirements and includes the purpose and applicability of the special publication. Chapter 2 describes the fundamentals of security certification and accreditation to include: (i) the roles and responsibilities of key participants; (ii) categories of information systems; (iii) the criteria for determining security accreditation boundaries; (iv) types of security accreditation decisions; (v) supporting documentation; and (vi) the process of continuous monitoring of security controls in information systems. Chapter 3 provides an overview of the different phases of the security certification and accreditation process and includes a brief description of the associated tasks and subtasks within each phase. The supporting annexes provide more detailed security certification and accreditation-related information to include references, definitions and terms, acronyms, a summary of roles and responsibilities, sample security accreditation decision letters, and a description of information security program activities.

CHAPTER TWO

2

THE FUNDAMENTALS

KEY PARTICIPANTS, ACCREDITATION BOUNDARIES, DECISIONS, AND DOCUMENTATION

"Outstanding agency security programs consider both technical and non-technical measures to build more secure systems, thus increasing the level of confidence individuals have in those systems."

The purpose of this chapter is to describe the fundamentals of security certification and accreditation to include: (i) roles and responsibilities of key participants; (ii) activities employed by the agency to verify security control effectiveness, determine information system vulnerabilities, and manage risk; (iii) categories of information systems; (iv) criteria used to determine security accreditation boundaries; (v) types of security accreditation decisions; (vi) documentation and supporting materials needed to successfully complete the process; and (vii) post accreditation activities employed by the agency to monitor the effectiveness of their security controls on an ongoing basis.

2.1 THE AGENCY PERSPECTIVE

When considering the prospect of certifying and accrediting agency information systems, it is important to put these activities into perspective with respect to the agency's mission and operational responsibilities. Employing more secure information systems is critical to the success of an agency in carrying out its mission and conducting its day-to-day functions. However, security is only one of many factors that must be considered by agency officials in the design, development, acquisition, operation, and maintenance of an information system. In the end, agencies must have information systems that provide a high degree of functionality and are sufficiently secure so as not to place undo risk on their respective missions. The cost of conducting security certifications and accreditations of large numbers of information systems across a range of complexity is a critical issue facing agencies. The solution to this problem can be found in part by: (i) adopting security certification and accreditation guidelines with simple well-defined tasks; (ii) reusing and sharing security certification and accreditation-related information (e.g., evaluation results, risk and vulnerability assessments) for similar agency information systems; and (iii) employing automated tools that help generate and facilitate the reuse and sharing of security certification and accreditation-related information. Cost savings can also be realized by employing "economies of scale" through the effective use of security accreditation boundaries as described in the next sections. And finally, reducing the cost of security certification and accreditation by taking advantage of standardized verification techniques and procedures in determining the effectiveness of security controls is another option available to agencies.

2.2 ROLES AND RESPONSIBILITIES

The following sections describe the roles and responsibilities of key participants involved in an agency's security certification and accreditation process.[12] Recognizing that agencies have widely varying missions and organizational structures, there may be differences in naming conventions for security certification and accreditation-related roles and how the associated responsibilities are allocated among agency personnel (e.g., multiple individuals filling a single role or one indi-

[12] Agencies may define other significant roles (e.g., information owners, information system security managers, facilities managers, security program managers, system security engineers, and operations managers) to support the security certification and accreditation process. The Office of the Inspector General may also become involved and take on the role of independent auditor in assessing the quality of the security certification and accreditation process.

vidual filling multiple roles). However, the basic security certification and accreditation functions remain the same. The security certification and accreditation process described in this special publication is flexible, allowing agencies to effectively carry out the specific tasks within their respective organizational structures to best manage the risks to the agency's operations and assets. A summary of the roles and responsibilities is provided in Annex D.

2.2.1 Authorizing Official

The *authorizing official* (or designated approving/accrediting authority as referred to by some agencies) is the senior management official or executive with the authority to approve the operation of the information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Through security accreditation, the authorizing official assumes responsibility and is accountable for the risks of operating the information system in a specific environment. The authorizing official should have the authority to oversee the budget and business operations of the information system within the agency and is often called upon to approve security requirements documents, security plans, memorandums of agreement (MOA), memorandums of understanding (MOU), and any authorized or allowable deviations from security policies. In addition to authorizing operation of an information system, the authorizing official can also: (i) issue an interim approval to operate the system under specific terms and conditions; or (ii) deny authorization to operate the system (or if the system is already operational, halt operations) if unacceptable security risks exist. With the increasing complexities of agency missions and organizations, it is possible that a particular information system may involve multiple authorizing officials. If so, agreements must be established among the authorizing officials and documented in the security plan. In most cases, it will be advantageous to agree to a lead authorizing official to represent the interests of the other authorizing officials.

2.2.2 Authorizing Official Designated Representative

Due to the breadth of organizational responsibilities and significant demands on time, the authorizing official cannot always be expected to participate directly in the planning and technical meetings that occur during the security certification and accreditation process. The authorizing official's *designated representative* is the agency staff member selected by the authorizing official to act on his or her behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of the information system. The authorizing official's designated representative interacts with the information system owner, information system security officer, certification agent, user representative, and other interested parties during the security certification and accreditation process. The designated representative can be empowered by the authorizing official to make certain decisions with regard to the planning and resourcing of the security certification and accreditation activities, the acceptance of the security plan, and the determination of residual risk to agency operations and assets. The designated representative may also be called upon to prepare the final security accreditation package, obtain the authorizing official's signature on the security accreditation decision letter, and transmit the accreditation package to the appropriate agency officials. The only activity that cannot be delegated to the authorizing official's designated representative is the security accreditation decision and the signing of the associated accreditation decision letter (i.e., the acceptability of residual risk to the agency). If a designated representative is not selected, the authorizing official is responsible for carrying out the activities described above.

2.2.3 Information System Owner

The *information system owner*[13] represents the interests of the user community throughout the life cycle of the information system. The information system owner is responsible for the development of the security plan and ensures the system is deployed and operated according to the security requirements documented in the plan. The system owner is also responsible for deciding who has access to the information system (and with what types of privileges or access rights) and ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior). The system owner informs key agency officials of the need to conduct a security certification and accreditation of the information system, ensures appropriate resources are available for the effort, and provides the necessary system-related documentation to the certification agent. The system owner receives the security test and evaluation results from the certification agent including: (i) an independent assessment of the effectiveness of the security controls in the information system; (ii) a description of the confirmed vulnerabilities in the system; and (iii) recommendations for corrective actions. After taking appropriate steps to reduce or eliminate vulnerabilities, the system owner assembles the final security certification package with inputs from the certification agent, information system security officer, and other interested parties and submits the package to the authorizing official or the authorizing official's designated representative.

2.2.4 Information System Security Officer

The *information system security officer* is the principal staff advisor to the system owner on all matters (technical and otherwise) involving the security of the information system. The information system security officer typically has the detailed knowledge and expertise required to manage the security aspects of the information system and, in many agencies, is assigned responsibility for the day-to-day security operations of the system. This responsibility may also include physical security, personnel security, incident handling, and security training and education. The information system security officer may be called upon to assist in the development of the system security policy and to ensure compliance with that policy on a routine basis. In close coordination with the information system owner, the information system security officer often plays an active role in developing and updating the security plan for the information system as well as in managing and controlling changes to the system and assessing the security impact of those changes.

2.2.5 Certification Agent

The *certification agent* is the individual responsible for conducting the comprehensive evaluation of the management, operational, and technical security controls in the information system to determine: (i) the effectiveness of those controls in a particular environment of operation; and (ii) the vulnerabilities in the system after the implementation of such controls. The certification agent also provides recommended corrective actions to reduce or eliminate vulnerabilities in the information system. Prior to initiating the security test and evaluation activities, the certification agent provides an independent assessment of the security plan to ensure the plan provides a complete and consistent security specification for the information system. Depending on the size and complexity of the information system and the needs of the agency, the certification agent may be supported by a certification team providing the essential assessment capabilities necessary to complete the evaluation of the security controls. To preserve the impartial and unbiased nature of the security certification, the certification agent should be in a position that is independent from the persons directly responsible for the development of the information system and the day-to-day

[13] The role of information system owner can be interpreted in a variety of ways depending on the particular agency and the life cycle phase of the information system. Some agencies may refer to information system owners as program managers or business/asset/mission owners.

operation of the system. The certification agent should also be independent of those individuals responsible for correcting security deficiencies identified during the security certification. The independence of the certification agent is an important factor in assessing the credibility of the security test and evaluation results and ensuring the authorizing official receives the most objective information possible in order to make an informed, risk-based security accreditation decision. The risk level of the information system (See Section 2.5) should guide the degree of independence of the certification agent. For low risk information systems, a self-assessment activity may be reasonable and appropriate and not require an independent certification agent. For all moderate and high risk information systems, a greater degree of certification agent independence is needed and justified.

2.2.6 User Representative

Users are found at all levels of an agency. Users are responsible for the identification of mission/operational requirements and the secure operation of a certified and accredited information system, based on the security plan. The *user representative* represents the operational interests and mission needs of the user community within the agency and serves as the liaison for that community throughout the life cycle of the information system. The user representative assists in the security certification and accreditation process, when needed, to ensure mission requirements are satisfied while meeting the security requirements and employing the security controls for the information system defined in the security plan.

2.2.7 Delegation of Roles

At the discretion of senior agency officials, certain security certification and accreditation roles may be delegated. Agency officials may appoint appropriately qualified individuals, to include contractors, to perform the activities associated with a particular security certification and accreditation role. The designated individuals are able to operate with the authority of the agency officials within the limits defined for the specific activities. Agency officials retain ultimate responsibility, however, for the results of actions performed by these delegated individuals. There is one exception to the delegation of roles. The role and signature responsibility of the authorizing official cannot be delegated to non-government personnel. The authorizing official role has inherent United States Government authority and can only be assigned to government personnel.

2.3 SECURITY CERTIFICATION AND ACCREDITATION

While security certification and accreditation are very closely related, they are indeed very distinct processes. Security accreditation is about the acceptance and management of risk—the risk to an agency's operations (including mission, functions, image, or reputation) or assets that results from the operation of an information system. Authorizing officials must be able to determine the residual risk to an agency's operations or assets and the acceptability of such risk given the confirmed vulnerabilities identified in their information systems and the mission or business needs of their enterprises. Authorizing officials weigh the appropriate factors and decide to either accept or reject the residual risk to their respective agencies. To ensure that authorizing officials make credible, risk-based decisions, several important questions must be answered during the security certification and accreditation process. A few of these key questions are listed below:

- Prior to the security certification being initiated, does the residual risk described in the security plan appear to be correct, and if so, would the risk be acceptable?
- After the security certification is completed, what are the confirmed vulnerabilities in the information system?

- What specific corrective actions have been taken or are planned to reduce or eliminate those vulnerabilities?
- How do the confirmed vulnerabilities in the information system translate into residual risk to agency operations or agency assets, and is this risk acceptable?

Security certification directly supports security accreditation by evaluating the security controls in the information system. This evaluation is conducted to determine the effectiveness of those security controls in a particular environment of operation and the vulnerabilities in the information system after the implementation of such controls. Security certification can include a variety of verification techniques and procedures to demonstrate the effectiveness of the security controls in the information system. These techniques and procedures can include such activities as observations, interviews, exercises, functional testing, penetration testing, regression testing, system design analysis, and test coverage analysis. The level of rigor applied during evaluation is based on the robustness of the security controls employed in the information system—where robustness is defined by the strength of the security controls and the assurance that the controls are effective in their operation.[14] Security certification does not include the determination of residual risk to agency operations or agency assets that may result from these information system vulnerabilities. The determination of residual risk to agency operations or agency assets generally requires a broader, more strategic view of the enterprise than can be obtained from the more technically focused, local view of the system that results from security certification. Authorizing officials and their designated representatives are better positioned to make residual risk determinations and the ultimate decisions on the acceptability of such risk. Authorizing officials or their designated representatives may, when needed, consult certification agents at any phase in the security certification and accreditation process to obtain technical advice on the security of the information system. Figure 2.1 illustrates the relationship between information system vulnerabilities (local view) and residual risk to agency operations or assets (strategic view).

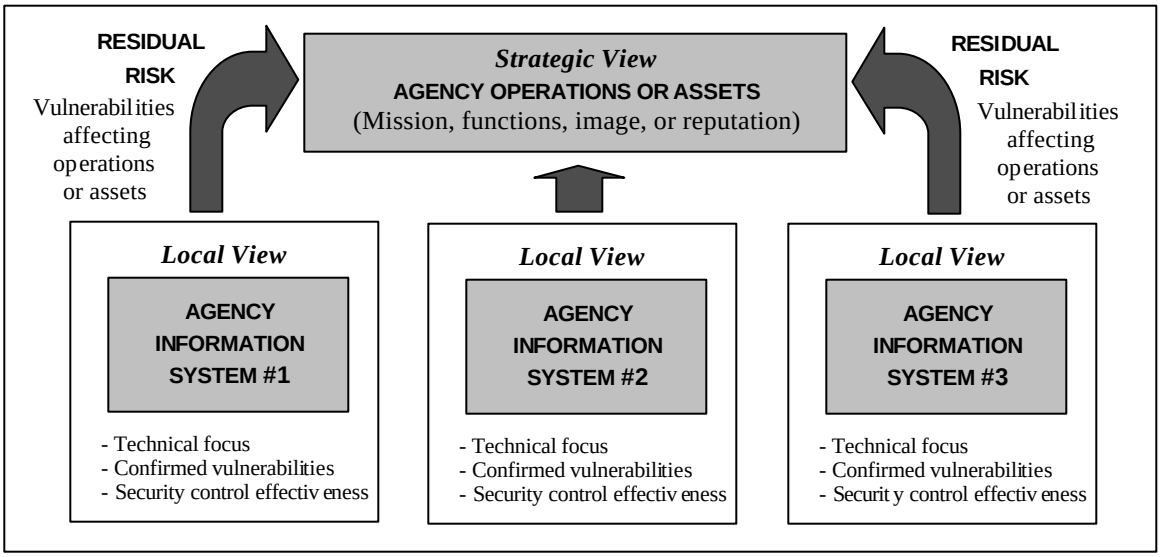

FIGURE 2.1 INFORMATION SYSTEM VULNERABILITIES AND RESIDUAL RISK

[14] Consult NIST Special Publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems*, (Initial public draft projected for publication, Winter 2003-04). These techniques and procedures, which are targeted toward the security controls defined in NIST Special Publication 800-53, *Security Controls for Federal Information Systems*, (Initial public draft projected for publication, Summer 2003), represent a baseline of assessment activity that can be supplemented by the agency, if necessary.

Security accreditation should not be viewed as a static process. An information system is authorized for operation at a specific point in time reflecting the current security state of the system. However, the inevitable changes to the hardware, firmware, and software in the information system and the potential impact those changes may have on the security of that system require a more dynamic process—a process capable of monitoring the ongoing effectiveness of the security controls in the information system. Thus, the initial security accreditation of the information system must be supplemented and reinforced by a structured and disciplined process involving: (i) the continuous monitoring of the security controls in the system; and (ii) the continuous reporting of the security state of the system to appropriate agency officials. The following questions should be answered during the information system monitoring process:

- Have any changes to the information system affected the current, documented vulnerabilities in the system?
- If so, has the residual risk to agency operations or assets been affected?
- Has a specified time period passed requiring the information system to be reauthorized in accordance with federal or agency policy?

The successful completion of the security certification and accreditation process provides agency officials with the necessary assurances that the information system has appropriate security controls and that any vulnerabilities in the system have been considered in the risk-based decision to authorize processing.

2.4 CATEGORIES OF INFORMATION SYSTEMS

All federal information systems have value and require some level of protection. FISMA requires the development of standards to be used by federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels.[15] FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Initial public draft), May 2003, establishes three potential levels of risk (low, moderate, and high) for each of the stated security objectives (confidentiality, integrity, and availability) relevant to securing federal information systems. The levels of risk consider both impact and threat, but are more heavily weighted toward impact. The impact is based on the potential magnitude of harm that the loss of confidentiality, integrity, or availability would have on agency operations (including mission, functions, image or reputation), agency assets, or individuals (including privacy). Threat information (including capability, intent, and resources of potential adversaries) for a specific information system is generally non-specific or incomplete at best. Recognizing the highly networked nature of the current federal computing environment, FIPS Publication 199 acknowledges the existence of baseline threats to all information systems. In other words, in today's interconnected and interdependent information systems

[15] It should be noted that OMB Circular A-130 implicitly associates levels of risk with different types of information systems and applications (e.g., major information systems, major applications, and general support systems). Based on the definitions provided in Circular A-130, agencies can associate the different types of information systems and applications with the security categories and risk levels defined in FIPS Publication 199. For example, a major information system (i.e., a system that requires special management attention because of its importance to an agency mission, its high development, operating, or maintenance costs, or its significant role in the administration of agency programs, finances, property, or other resources) could be expected to have a risk level of moderate or high. Similarly, a major application (i.e., an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application) could also be expected to have a risk level of moderate or high. And finally, a general support system could be expected to have a risk level of low, moderate, or high depending on the importance of the system, potential impact of loss, and whether the system is supporting (i.e., hosting) any major applications.

environment, which encompasses many common platforms and technologies, there is a high likelihood of a variety of common threats (both intentional and unintentional) acting to compromise the security of information systems. Accordingly, the levels of risk focus on what is known about the potential impact or harm that could arise if certain events occur and the information and information system are not available to accomplish the agency's assigned mission, preserve its image or reputation, protect its assets, maintain its day-to-day functions and protect individuals.

Security categories and the associated risk levels described in FIPS Publication 199 play an important part in the security certification and accreditation of an information system. Risk levels are typically considered during the risk assessment to help guide the selection of security controls for an information system. Minimum security controls as defined in NIST Special Publication 800-53, *Security Controls for Federal Information Systems* (Initial public draft projected for publication, Summer 2003), serve as a baseline, or starting point for agencies in determining the security controls necessary to protect their information systems. In addition to the selection of security controls, the risk levels may also affect the rigor of the testing and evaluation techniques and procedures used to verify the effectiveness of the security controls during the security certification process. Security categorization standards for federal information systems provide a common framework and understanding that promotes: (i) effective government-wide management and oversight of federal agency information security programs, including the coordination of information security efforts throughout the civilian, national security, and law enforcement communities; and (ii) consistent agency reporting to OMB and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.

2.5 SECURITY ACCREDITATION BOUNDARIES

One of the most difficult and challenging problems for agencies has been identifying appropriate security accreditation boundaries for their information systems. Security accreditation boundaries for agency information systems need to be established during the initial assessment of risk and development of security plans. Boundaries that are too expansive make the security certification and accreditation process extremely unwieldy and complex. Boundaries that are too limited increase the number of security certifications and accreditations that must be conducted and thus, drive up the total security costs for the agency. While there are no specific rules for determining security accreditation boundaries for information systems, there are, however, some guidelines and considerations described in the following sections that may be helpful to agencies in making boundary determination tasks more manageable.

2.5.1 Establishing Information System Boundaries

The process of uniquely assigning information resources[16] to information systems defines the security accreditation boundaries of each system. In general, if a set of information resources is identified as an information system, the resources should meet the following criteria: (i) be under the same direct management control;[17] (ii) have the same function or mission objective; (iii) have essentially the same operating characteristics and security needs; and (iv) reside in the same general operating environment (or in the case of a distributed information system, reside in various

[16] Information resources consist of information and related resources, such as personnel, equipment, funds, and information technology.

[17] Direct management control typically involves budgetary, programmatic, or operational authority and associated responsibility. For new information systems, management control can be interpreted as having budgetary/programmatic authority and responsibility for the development and deployment of the information systems. For information systems currently in the federal inventory, management control can be interpreted as having budgetary/operational authority for the day-to-day operations and maintenance of the information systems.

locations with similar operating environments). The application of the criteria results in the assignment of a security accreditation boundary to a single information system. There are certain situations when management span of control and information system boundaries can be used to streamline the security certification and accreditation process, and thus increase its overall cost effectiveness. The following section describes two such situations.

2.5.2 Using Boundaries to Facilitate Reuse of Security Evaluation Results

There are many ways to reduce the cost of security certification and accreditation by reusing and sharing security evaluation results. One such approach involves an information system that is targeted for deployment and installation at multiple sites (e.g., a standard financial system or standard personnel management system). The information system usually consists of a common set of hardware, software, and firmware. Since it is often difficult and costly to accredit a common information system at all possible sites, the process can be streamlined by reusing security evaluation results. To effectively reuse security evaluation results, it is first necessary to partition the security controls in the information system into two classes: (i) *system-specific* controls; and (ii) *site-specific* controls. System-specific security controls (e.g., access controls, identification and authentication controls, audit controls, cryptographic controls) are those controls that can be fully evaluated during an initial security certification prior to the information system being deployed to its operational environment. This preliminary security evaluation (also referred to as *type certification*) often occurs at a central integration and test facility or at one of the intended operating sites, if an integration and test facility is not available. Site-specific security controls (e.g., personnel security controls, physical security controls) are those controls that have an operational context or some identifiable dependency on the physical location or site where the information system is to be deployed and operated. The evaluation of site-specific security controls must be deferred until the information system is delivered and installed at its final destination. This follow-on security evaluation occurs at each location or site where the information system resides. In the situation described above, where a common information system is being deployed at multiple sites, the agency can take advantage of reusing security evaluation results by evaluating the system-specific security controls one time at the central integration and test facility and reusing the results when the information system goes through its security accreditation at the respective operational sites.

A second approach that can be used to reduce security certification and accreditation costs involves multiple information systems contained within a single facility or located at a centralized site. The information systems may be grouped together when there are several agency organizations in a self-contained location within a proximate geographic area and the organizations serve under the same executive, face common threats, share a common mission, and have comparable vulnerabilities. It is often a waste of valuable resources to evaluate security controls (common to all information systems at the site) multiple times. The process can be streamlined by reusing security evaluation results of the common site-specific controls (also referred to as *site certification*). The site-specific security controls common to all information systems are evaluated one time during the site certification and the results subsequently shared among all information systems at the site. The security certification and accreditation process is completed on each information system at the site with significant reuse of security evaluation results from the site-specific security controls. The results from any reevaluation of site-specific controls should be shared and incorporated into the security certification and accreditation documentation of all information systems at the site.

The two situations described above promote both the reuse and sharing of security evaluation results—the first example focusing on the reuse of security evaluation results from system-specific security controls and the second example focusing on the reuse of security evaluation results from

site-specific security controls. In both cases, the security certification process is made more efficient by the reuse and sharing of security evaluation results, as appropriate, and makes the final security accreditations of the individual information systems more cost effective. Figure 2.2 illustrates the concept of reuse of security evaluation results.

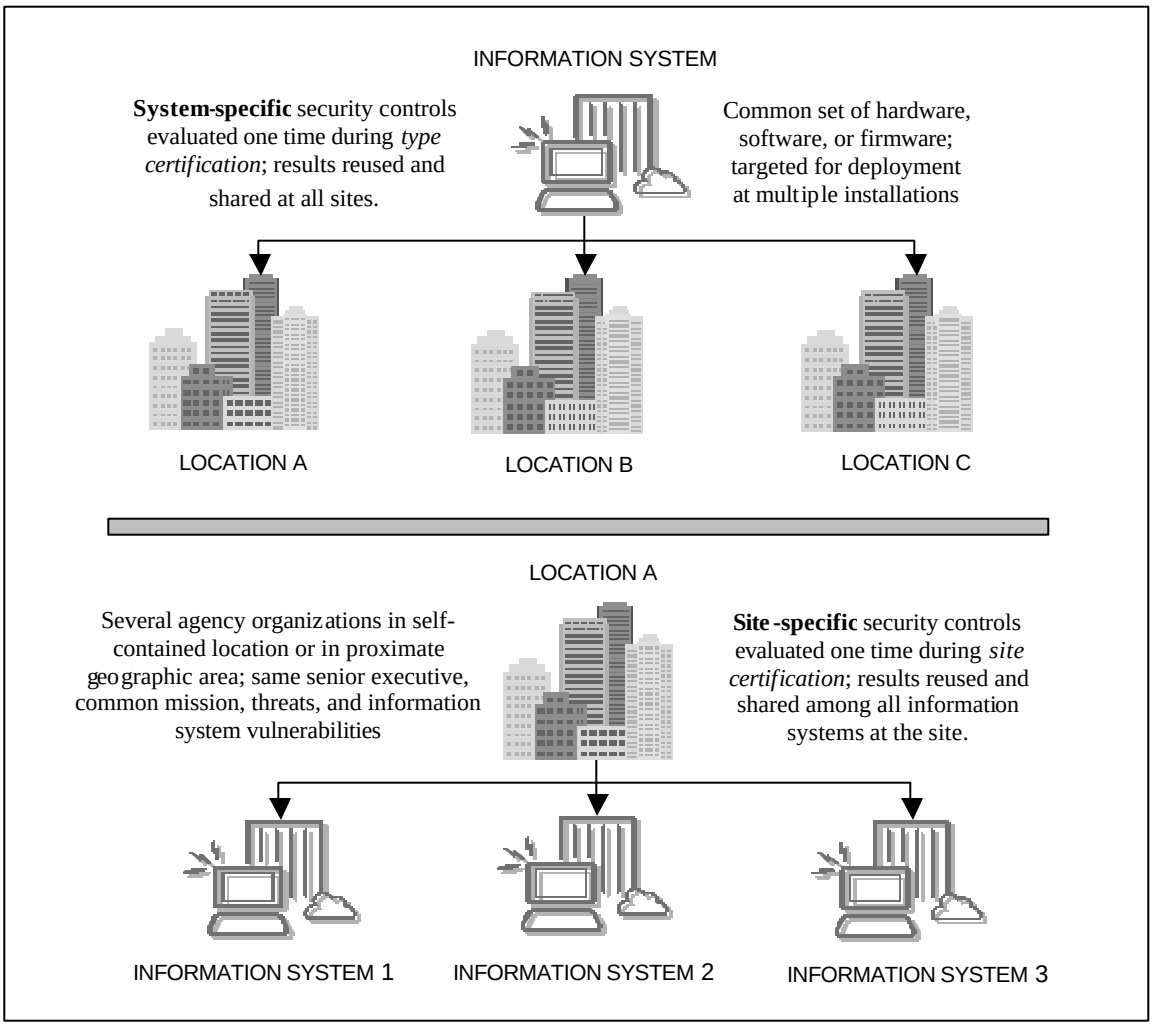

FIGURE 2.2 REUSE OF SECURITY EVALUATION RESULTS

2.5.3 Large and Complex Information Systems

The application of security controls uniformly across large and complex information systems may be cost prohibitive and technically infeasible for the agency. Accordingly, any attempt to test and evaluate the security controls in such systems may also be cost prohibitive and unrealistic. To make this problem more manageable, authorizing officials should examine the nature of the information systems being considered for security certification and accreditation and the feasibility of decomposing the systems into more manageable components. The decomposition of large and complex systems into multiple components, or *subsystems*,[18] facilitates the application of the security certification and accreditation process in a more cost effective manner and supports the concepts of risk management and defense-in-depth. A defense-in-depth strategy recognizes that

[18] A subsystem is a major subdivision or component of an information system consisting of hardware, software, or firmware that performs a specific function.

an information system can be viewed as a wide-ranging interconnected, end-to-end set of information capabilities managed as a single enterprise. Accordingly, for a large and complex information system, an authorizing official, in consultation and coordination with the system owner, may define subsystem components with established subsystem boundaries. The decomposition into subsystem components should be reflected in the security plan for that information system. Each subsystem component is fully characterized in the security plan, an appropriate risk level assigned, (See FIPS Publication 199) and a set of security controls identified. Thus, the selection and employment of appropriate sets of security controls in the various subsystems (e.g., security controls for low risk, moderate risk, or high risk systems) and the application of appropriate techniques and procedures to determine the effectiveness of those controls can facilitate a more cost effective security certification and accreditation process.

To illustrate a simple example of system decomposition, an information system contains a system guard that monitors the flow of information between two local area networks. The information system, in this case, can be partitioned into three subsystem components: (i) local area network Alpha; (ii) local area network Bravo; and (iii) the system guard separating the two networks. Local area network Alpha is a high risk subsystem component for confidentiality.[19] Local area network Bravo is a moderate risk subsystem for confidentiality. The guard subsystem must be highly trusted to do its assigned security tasks (i.e., only letting certain information pass between the respective networks) and is therefore, a high risk subsystem component for confidentiality. The security controls employed in the particular subsystems are commensurate with their respective (FIPS Publication 199) risk levels. The testing and evaluation techniques and procedures employed to determine the effectiveness of the security controls in the guard and local area network Alpha subsystems will be more rigorous and extensive than the techniques and procedures employed to determine the effectiveness of the security controls in the local area network Bravo subsystem. Figure 2.3 illustrates the concept of information system decomposition and the security certification and accreditation process for a large and complex agency system.

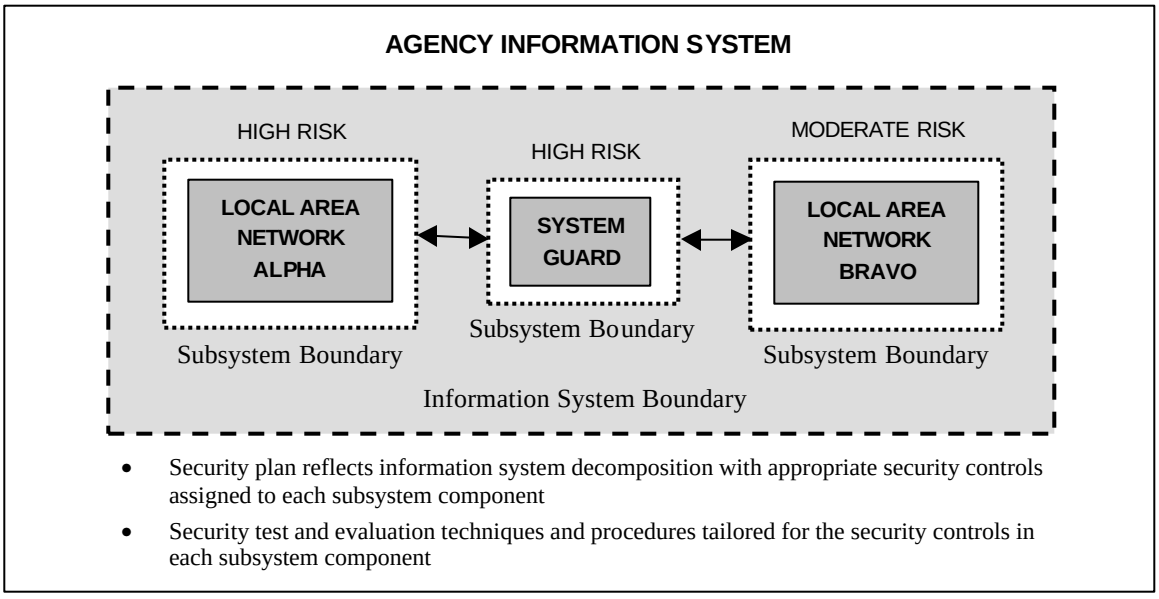

FIGURE 2.3 DECOMPOSITION OF LARGE AND COMPLEX INFORMATION SYSTEMS

[19] Risk levels are described in FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Initial public draft), May 2003.

2.6 SECURITY ACCREDITATION DECISIONS

Security accreditation decisions convey the results of security certification and accreditation processes to information system owners. A security accreditation decision can be made only after a security certification is completed. There are three types of security accreditation decisions that can be rendered by authorizing officials; (i) full authorization to operate; (ii) interim approval to operate; and (iii) denial of authorization to operate. Each of these security accreditation decisions is described below. Sample security accreditation decision letters are provided in Annex E.

2.6.1 Full Authorization to Operate

If, after assessing the results of the security certification, the residual risk to the agency's operations or assets is deemed fully acceptable to the authorizing official, a full authorization to operate is issued for the information system. The information system is accredited without any significant restrictions or limitations on its operation. Although not affecting the security accreditation decision for full authorization to operate, authorizing officials may recommend specific actions be taken to reduce or eliminate identified vulnerabilities, where it is cost effective to do so. A disciplined and structured process should be established by the agency to monitor the effectiveness of the security controls in the information system on an ongoing basis (See Section 2.8). Security reaccreditation occurs at the discretion of the authorizing official in accordance with federal or agency policy— typically when significant changes have taken place in the information system or when a specified time period has elapsed (e.g., every three years).

2.6.2 Interim Approval to Operate

If, after assessing the results of the security certification, the residual risk to the agency's operations or assets is not deemed fully acceptable to the authorizing official, but there is an overarching need to place the information system into operation or continue its operation due to mission necessity, an interim approval to operate may be issued. An interim approval provides a limited authorization to operate the information system under specific terms and conditions and acknowledges greater risk to the agency's operations and assets for a limited period of time. The terms and conditions, established by the authorizing official, convey limitations on information system operations. The information system is *not* considered accredited during the period of limited authorization to operate. The maximum allowable timeframe for an interim approval to operate should be commensurate with the risk level associated with the information system.[20] For a low risk system, an interim approval to operate should be issued for a maximum time period of one year; for a moderate risk system, an interim approval to operate should be issued for a maximum time period of six months; and, for a high risk system, an interim approval to operate should be issued for a maximum time period of ninety days. At the end of the period of limited authorization, the information system should either meet the requirements for being fully authorized or not be authorized for further operation. Renewals or extensions to interim approvals to operate should be discouraged and approved by authorizing officials only under the most extreme or extenuating of circumstances. A disciplined and structured process must be established by the agency to monitor the effectiveness of the security controls in the information system during the period of limited authorization. Monitoring activities should focus on the specific vulnerabilities in the information system identified during the security certification. Significant changes in the security

[20] Risk levels are described in FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Initial public draft), May 2003.

state of the information system that occur during the period of limited authorization should be reported immediately to the authorizing official.

2.6.3 Denial of Authorization to Operate

If, after assessing the results of the security certification, the residual risk to the agency's operations or assets is deemed unacceptable to the authorizing official, the authorization to operate the information system is denied. The information system is not accredited and should not be placed into operation—or for an information system currently in operation, all activity should be halted. Failure to receive authorization to operate or an interim approval to operate usually indicates that there are major deficiencies in the security controls in the information system. The authorizing official or designated representative should work with the information system owner to revise the plan of action and milestones to ensure that proactive measures are taken to correct the security deficiencies in the information system.

2.6.4 Agency-wide Issues Affecting Security Accreditation

Some of the deficiencies in security controls noted during the security certification of the information system (e.g., problems with the physical security of the system or shortcomings in the security training program), might represent agency-wide deficiencies that could be indicative of systemic problems in the agency information security program. These types of agency-wide deficiencies will, in all likelihood, appear in the security certifications of other information systems within the agency. Authorizing officials should view these types of deficiencies as early warning signs and take the appropriate steps to correct the noted problems.

In the event that a new authorizing official is assigned responsibility for the information system, the most recent security accreditation (i.e., security accreditation decision, decision rationale, and terms and conditions) completed by the agency remains in effect and is valid until the new authorizing official directs that a reaccreditation action be initiated. Newly assigned authorizing officials may wish to review the current security certification and accreditation packages and the current status reports from the continuous monitoring process to determine if any such security reaccreditation action is warranted. The willingness of the new authorizing official to accept the residual risk to the agency's operations or assets as stated in the current security accreditation package is a key factor in the decision on whether or not a reaccreditation action is needed.

2.7 SUPPORTING DOCUMENTATION

There are two documents that are essential to completing the security certification and accreditation process: (i) the security certification package; and (ii) the security accreditation package. The purpose and content of these packages are described in the following sections.

2.7.1 Security Certification Package

The security certification 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. The information system owner is responsible for the assembly and compilation of the final security certification package with inputs from the information system security officer and the certification agent. The security certification package contains the following documents: (i) the updated security plan; (ii) the security test and evaluation report; and (iii) the plan of action and milestones. The security plan is updated by the information system owner based on the results of the security certification. The security test and evaluation report, prepared by the certification agent, provides the results of the independent testing and evaluation of the security controls in the information system, a description of

the confirmed vulnerabilities in the system, and a list of recommended corrective actions. The plan of action and milestones, prepared by the system owner, indicates corrective actions taken or planned to reduce or eliminate the identified vulnerabilities in the information system. The final security certification package is submitted to the authorizing official or designated representative by the information system owner. Figure 2.4 illustrates the key sections of the security certification package.

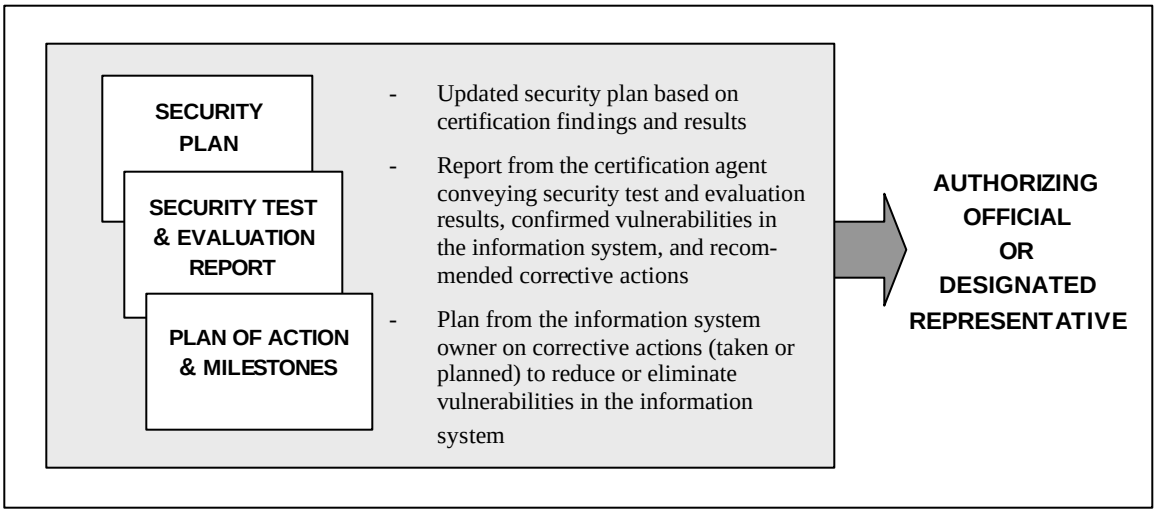

FIGURE 2.4 CONTENTS OF THE SECURITY CERTIFICATION PACKAGE

2.7.2 Security Accreditation Package

The security accreditation package transmits the security accreditation decision from the authorizing official to the information system owner. The authorizing official's designated representative or support staff prepares the final security accreditation package for the authorizing official with decision recommendations, as appropriate. The security accreditation package contains the following information: (i) the security accreditation decision letter signed by the authorizing official conveying the accreditation decision, supporting rationale for the decision, and any terms and conditions placed on the system owner; and (ii) any supporting documentation related to the security certification and accreditation process that the authorizing official wishes to provide to the system owner. Figure 2.5 illustrates the key sections of the security accreditation package.

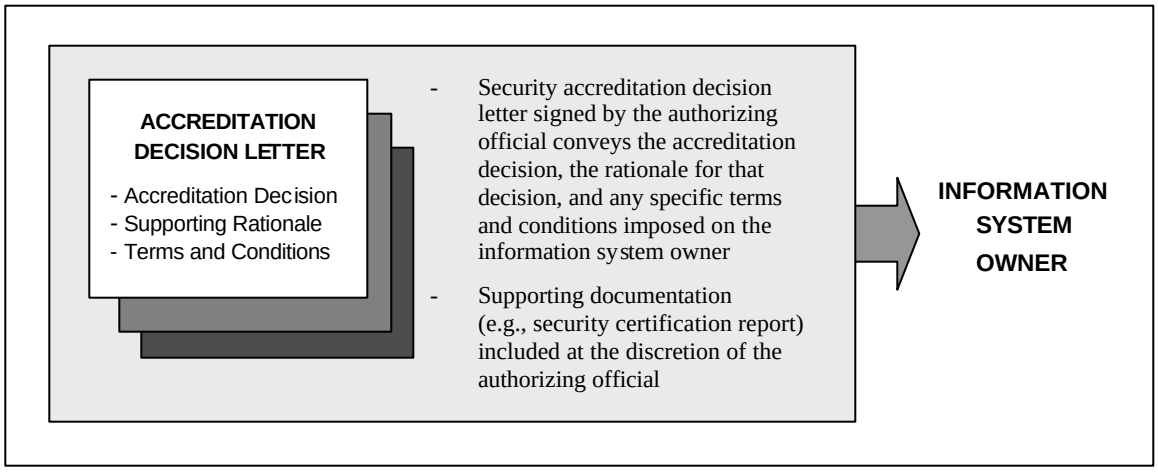

FIGURE 2.5 CONTENTS OF THE SECURITY ACCREDITATION PACKAGE

The contents of security certification and accreditation-related documentation (especially information dealing with information system vulnerabilities) should be marked and protected appropriately in accordance with agency policy.

2.8 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 monitoring program requires: (i) a structured and disciplined configuration management and control process; (ii) a process to verify the continued effectiveness of the security controls in the information system; and (iii) procedures to report the security status of the system to appropriate agency officials. With regard to configuration management and control, it is important to document the proposed or actual changes to the information system and to subsequently determine the impact of those proposed or actual changes on the security of the system. Information systems will typically be in a constant state of migration with upgrades to hardware, software, or firmware and possible modifications to the surrounding environment where the system resides. Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation.

Realizing that it is not feasible or cost-effective to evaluate all of the security controls in the information system on an ongoing basis, the agency should select an appropriate subset of those controls for periodic testing and evaluation. The criteria established by the agency for selecting which security controls will be monitored should reflect the agency's priorities and importance of the information system to its operations (including mission, functions, image, or reputation) and assets. The authorizing official (or designated representative) and information system owner, in consultation with the information system security officer, should agree on the set of security controls in the information system that are to be monitored on an ongoing basis as well as the frequency of such monitoring activity.

The results of the continuous monitoring activity should be documented in the security plan for the information system and reported to the authorizing official or authorizing official's designated representative on a regular basis. The security plan should contain the most up-to-date information about the information system since the authorizing official, information system owner, information system security officer, and certification agent will be using the plan to guide any future security certification and accreditation activities, when required. The security status report should describe the continuous monitoring activities employed by the agency and include a plan of action and milestones from the information system owner. The plan of action and milestones address vulnerabilities in the information system discovered during the security impact analysis or security control monitoring and how the system owner intends to deal with those vulnerabilities (i.e., reduce, eliminate, or accept the vulnerabilities). The ongoing monitoring of security controls in the information system continues until the need for security reaccreditation occurs, either because of specific changes to the system (event-driven) or because of federal or agency policies requiring reauthorization of the system at a specified timeframe.

CHAPTER THREE

3

THE CERTIFICATION AND ACCREDITATION PROCESS

PHASES, TASKS AND DELIVERABLES

"Assurance is the degree of confidence one has that the security controls in an agency's information system work as intended to protect the system and the information it processes, stores, and transmits."

The security certification and accreditation process consists of four distinct phases: (i) an Initiation Phase; (ii) a Security Certification Phase; (iii) a Security Accreditation Phase; and (iv) a Continuous Monitoring Phase. Each phase consists of a set of well-defined tasks and subtasks that are to be carried out by the authorizing official, authorizing official's designated representative, information system owner, information system security officer, certification agent, and user representative. The security certification and accreditation activities can be applied to an information system at appropriate phases in the system development life cycle by selectively tailoring the various tasks and subtasks. Figure 3.1 provides a high level view of the security certification and accreditation process including the tasks associated with each phase in the process.

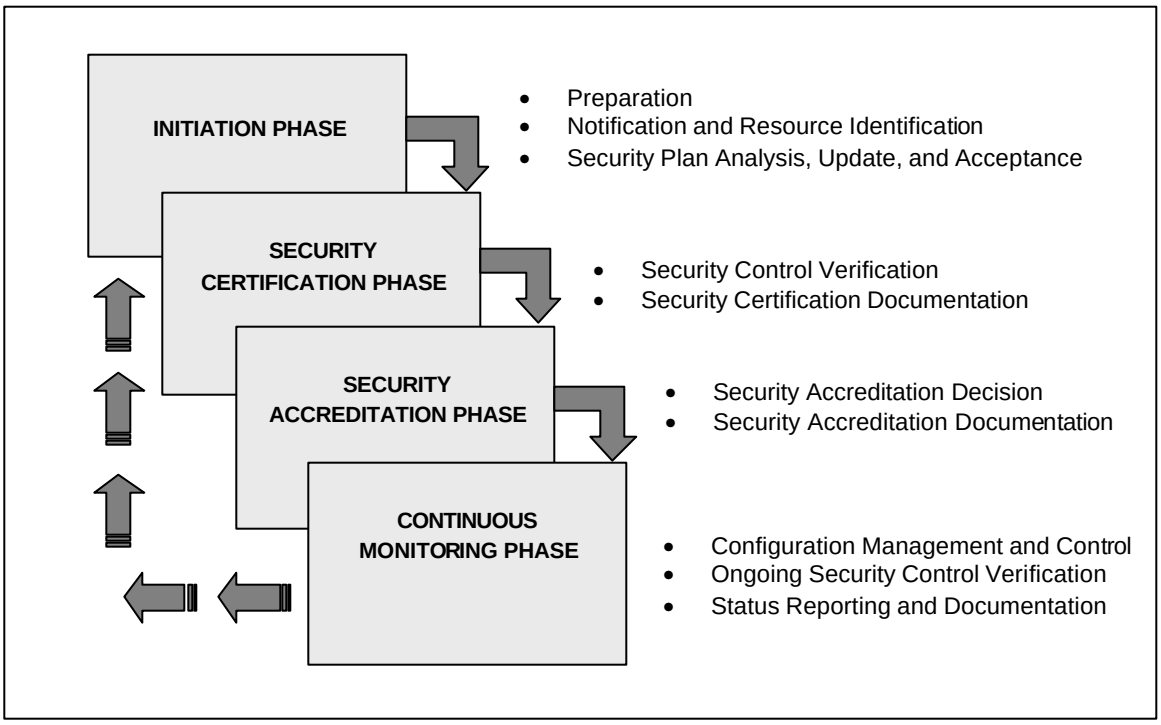

FIGURE 3.1 SECURITY CERTIFICATION AND ACCREDITATION PROCESS

3.1 INITIATION PHASE

The Initiation Phase consists of three tasks: (i) preparation; (ii) notification and resource identification; and (iii) security plan analysis, update, and acceptance. The purpose of this phase is to ensure that the authorizing official or designated representative is in agreement with the contents of the security plan for the information system before the certification agent begins the independent testing and evaluation of security controls. The early involvement of the authorizing official or designated representative with key participants such as the information system owner, information system security officer, certification agent, and user representative is paramount to the suc-

cess of the security certification and accreditation effort. A significant portion of the information needed during the Initiation Phase should have been previously generated by the agency during the initial assessment of risk and the subsequent development of the security plan for the information system. In many cases, risk assessments and security plans have been reviewed and approved by agency officials. If so, the subtasks in Task 1 (preparation task) should be reviewed to ensure all were completed at an earlier time. If an agency has not completed a risk assessment and a security plan, those activities should be completed prior to proceeding with the security certification and accreditation process.

TASK 1: PREPARATION

The objective of this task is to prepare for security certification and accreditation by reviewing the security plan for the information system and confirming that the contents of the plan are consistent with an initial assessment of risk.

SYSTEM DESCRIPTION

SUBTASK 1.1: Confirm that the information system has been fully characterized and documented in the security plan or an equivalent document.

RESPONSIBILITY: [Information System Owner]

ADVISORY NOTE: A typical system description includes: (i) the name of the information system; (ii) a unique identifier for the information system; (iii) the status of the information system with respect to the system development life cycle; (iv) the name and location of the agency responsible for the information system; (v) contact information for the information system owner or other individuals knowledgeable about the information system; (vi) contact information for the individual(s) responsible for security of the information system; (vii) the mission of the information system (i.e., purpose, functions, and capabilities); (viii) the types of information processed, stored, and transmitted by the information system; (ix) the boundary of the information system for operational authorization (or security accreditation); (x) the functional requirements of the information system; (xi) the applicable laws, directives, regulations, standards, or policies affecting the security of the information and the information system; (xii) the individuals who use and support the information system (including their organizational affiliations, access rights, privileges, and citizenship, if applicable); (xiii) the architecture of the information system; (xiv) hardware and firmware devices (including wireless and RF); (xv) system and applications software (including mobile code); (xvi) hardware, software, and system interfaces (internal and external); (xvii) information flows (i.e., inputs and outputs); (xviii) the network topology; (xix) network connection rules for communicating with external information systems; (xx) interconnected information systems and unique identifiers for those systems; (xxi) encryption techniques used for information processing, transmission, and storage; (xxii) public key infrastructures, certificate authorities, and certificate practice statements; (xxiii) the physical environment in which the information system operates; and (xxiv) web protocols and distributed, collaborative computing environments (processes, and applications). Descriptive information about the information system is typically documented in the system identification section of the security plan or in some cases, included in attachments to the plan. System identification information can also be provided by referencing appropriate documents. The level of detail depends on the availability of information to the agency.

REFERENCES: [NIST Special Publications 800-18, 800-30 or equivalents]

SECURITY CATEGORIZATION

SUBTASK 1.2: Confirm that the security category of the information system has been determined and documented in the security plan or an equivalent document.

RESPONSIBILITY: [Information System Owner]

ADVISORY NOTE: FIPS Publication 199 establishes three risk levels (low, moderate, and high) for each of the stated security objectives (confidentiality, integrity, and availability) relevant to securing federal information systems. The risk level of the information system focuses on the potential impact and magnitude of harm that the loss of confidentiality, integrity, or availability would have on agency operations (including mission, functions, image, or reputation) or agency assets. It is recognized that an information system may contain more than one type of information, (e.g., privacy information, medical information, proprietary information, financial information, contractor sensitive information, system security information), each of which is subject to security categorization. The security categorization of an information system that processes, stores, or transmits multiple types of information should be at least the highest risk level that has been determined for each type of information for each security objective of confidentiality, integrity, and availability. The security category should be considered during the risk assessment to help guide the agency's selection of security controls for the information system. Security categorization information is typically documented in the system identification section of the security plan or included as an attachment to the plan.

REFERENCES: [FIPS Publication 199, NIST Special Publications 800-18, 800-30 or equivalents]

THREAT IDENTIFICATION

SUBTASK 1.3: Confirm that potential threats that could exploit information system flaws or weaknesses have been identified and documented in the security plan or an equivalent document.

RESPONSIBILITY: [Information System Owner]

ADVISORY NOTE: It is important to consider all potential threats that could cause harm to an information system, ultimately affecting the confidentiality, integrity, or availability of the system. Threats can be natural, (floods, earthquakes, tornadoes, landslides, avalanches, electrical storms), human, (events that are either enabled by or caused by human beings), or environmental, (long-term power failures, pollution, chemicals, liquid leakage). It should be noted that not all possible threats that might be encountered in the environment need to be listed—only those that are relevant to the security of the information system. Threat information (including capabilities, intentions, and resources of potential adversaries) for a specific information system is generally non-specific or incomplete at best. Recognizing the highly networked nature of the current federal computing environment, there exists an acknowledged set of baseline threats to all information systems. In other words, in today's interconnected and interdependent information systems environment, which encompasses many common platforms and technologies, there is a high likelihood of a variety of threats (both intentional and unintentional) acting to compromise the security of agency information systems. In addition to this generalized assumption about threats, specific threat information, if available, should be used during the risk assessment to help guide the agency's selection and implementation of security controls for the information system. Threat identification information is typically documented in the

risk assessment report, which should be included in the security plan., either by reference or as an attachment.

REFERENCES: [NIST Special Publications 800-18, 800-30, or equivalents]

SECURITY CONTROL IDENTIFICATION

SUBTASK 1.4: Confirm that the security controls (either planned or implemented) for the information system have been identified and documented in the security plan or an equivalent document.

RESPONSIBILITY: [Information System Owner]

ADVISORY NOTE: Minimum security controls for low, moderate, and high risk information systems are listed in NIST Special Publication 800-53, *Security Controls for Federal Information Systems*, (Initial public draft projected for publication, Summer 2003). These predefined sets of security controls (geared to the risk levels defined in FIPS Publication 199), provide a baseline, or starting point, for agencies in addressing the necessary safeguards and countermeasures required for their information systems. The minimum security controls for low, moderate, and high risk information systems have specific assumptions about classes of threats that might be adequately countered by the baseline controls at each risk level. Agencies should perform additional analyses to determine if adjustments to the baseline set of security controls are needed. These adjustments to the baseline set of security controls may take the form of adding supplemental security controls or eliminating certain security controls based on specific threat and vulnerability information generated during the risk assessment for the information system and the agency's determination of acceptable level of risk. Adjustments to the baseline set of security controls should be reasonable, appropriate, and fully documented in the security plan with supporting rationale. Upon completion of the security control identification process, the agreed upon set of controls, taken together, should satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information. Security control information is typically documented in the management, operational, and technical controls section of the security plan.

REFERENCES: [NIST Special Publications 800-18, 800-30, 800-53 or equivalents]

VULNERABILITY IDENTIFICATION

SUBTASK 1.5: Confirm that flaws or weaknesses in the information system that could be exploited by potential threats have been identified and documented in the security plan or an equivalent document.

RESPONSIBILITY: [Information System Owner]

ADVISORY NOTE: Flaws or weaknesses in an information system that could be exploited by potential threats determine the potential vulnerabilities in that system. Vulnerability identification can be conducted at any phase in the system development life cycle. If the system is under development, the search for vulnerabilities focuses on the organization’s security policies, planned security procedures, system requirement definitions, and developer security product analyses. If the system is being implemented, the identification of vulnerabilities is expanded to include more specific information, such as the planned security features described in the security design documentation and the results of the developmental security test and evaluation. If the system is operational, the process of identifying vulnerabilities includes an analysis of the system security controls employed to protect the system. The identification

of vulnerabilities can be accomplished in a variety of ways using questionnaires, on-site interviews, document reviews, and automated scanning tools. Vulnerability sources include, for example: (i) previous risk assessment documentation; (ii) audit reports; (iii) system anomaly reports; (iv) security reviews; (v) self assessments; (vi) results of vulnerability scans and penetration tests; (vii) security test and evaluation reports; (viii) vulnerability lists; (ix) security advisories; (x) vendor advisories; (xi) commercial computer incident/emergency response teams and post lists; (xii) information security vulnerability alerts and bulletins; and (xiii) hardware, software, or firmware security analyses. Vulnerability identification information is typically documented in the risk assessment report, which should be included in the security plan, either by reference or as an attachment.

REFERENCES: [NIST Special Publications 800-18, 800-30 or equivalents]

RESIDUAL RISK DETERMINATION (EXPECTED)

SUBTASK 1.6: Confirm that the expected residual risk to agency operations or agency assets has been determined and documented in the security plan or an equivalent document.

RESPONSIBILITY: [Information System Owner, Information System Security Officer]

ADVISORY NOTE: FISMA and OMB Circular A-130 require an assessment of risk as part of a risk-based approach to determining adequate, cost-effective security for an information system. The methods used to assess risk should include consideration of the major factors in risk management including: (i) threats to and vulnerabilities in the information system; (ii) potential impact and magnitude of harm to the agency's operations (including mission, functions, image, or reputation) or assets that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and the information system; and (iii) the effectiveness of current or proposed security controls. It is impractical, in most cases, to plan for or implement security controls that address all potential vulnerabilities. The expected vulnerabilities are those vulnerabilities projected to remain in the information system after the employment of the planned or implemented security controls. Expected vulnerabilities resulting from the ineffectiveness or absence of security controls (i.e., controls *not* implemented) provide the basis for determining the expected residual risk to agency operations or assets posed by the operation of the information system. Assessing risk should be an ongoing activity to ensure that new threats and vulnerabilities are identified and appropriate security controls are implemented. Residual risk is typically documented in the risk assessment report, which should be included in the security plan, either by reference or as an attachment.

REFERENCE: [FISMA, OMB Circular A-130, NIST SP 800-30 or equivalent]

TASK 2: NOTIFICATION AND RESOURCE IDENTIFICATION

The objective of this task is to: (i) provide notification to all concerned agency officials as to the need for security certification and accreditation of the information system; (ii) determine the resources needed to carry out the effort; and (iii) prepare a plan of execution for the security certification and accreditation activities indicating the proposed schedule and key milestones.

NOTIFICATION

SUBTASK 2.1: Inform the authorizing official, certification agent, user representative, and cognizant agency officials that the information system will require security certification and accreditation support.

RESPONSIBILITY: [Information System Owner]

ADVISORY NOTE: The initial notification of key agency officials is an important activity to establish the security certification and accreditation process as an integral part of the system development life cycle. The notification also serves as an early warning to help prepare potential participants for the upcoming tasks that will be necessary to plan, organize and conduct the security certification and accreditation.

REFERENCE: [OMB Circular A-130]

PLANNING AND RESOURCES

SUBTASK 2.2: Determine the level of effort and resources required for the security certification and accreditation of the information system (including organizations involved) and prepare a plan of execution.

RESPONSIBILITY: [Authorizing Official or Designated Representative, Information System Owner, Certification Agent]

ADVISORY NOTE: The level of effort required for security certification and accreditation depends in large part, on three factors: (i) the size and complexity of the information system; (ii) the security controls employed to protect the system (e.g., the minimum security controls from NIST Special Publication 800-53 recommended for FIPS Publication 199 risk levels and any subsequent agency adjustments to that baseline set of controls); and (iii) the specific techniques and procedures used to verify the effectiveness of the security controls (e.g., the verification techniques and procedures from NIST Special Publication 800-53A). Identifying appropriate resources (e.g., supporting organizations, funding, and individuals with critical skills) needed for the security certification and accreditation effort is an essential aspect of the initial preparation activities. Once a certification agent is selected (or certification services procured), an execution plan for conducting the security certification and accreditation is prepared by the certification agent and approved by the system owner and the authorizing official or designated representative. An execution plan contains specific tasks, milestones, and delivery schedule.

REFERENCE: [OMB Circular A-130]

TASK 3: SECURITY PLAN ANALYSIS, UPDATE, AND ACCEPTANCE

The objective of this task is to: (i) obtain an independent analysis of the security plan; (ii) update the security plan as needed based on the results of the independent analysis; and (iii) obtain acceptance of the security plan by the authorizing official or designated representative prior to security testing and evaluation. The completion of this task will conclude the Initiation Phase of the security certification and accreditation process.

SECURITY PLAN ANALYSIS

SUBTASK 3.1: Analyze the security plan to determine if the expected vulnerabilities in the information system and the resulting expected residual risk to agency operations (including mission, functions, image, or reputation) or agency assets, is actually what the plan would produce.

RESPONSIBILITY: [Certification Agent, Authorizing Official or Designated Representative]

ADVISORY NOTE: The security plan serves as the primary roadmap or security specification for the information system. The independent review of the security plan by the

certification agent and authorizing official or designated representative determines if the plan is complete and consistent. The certification agent and authorizing official or designated representative also determine, at the level of analysis possible with only available planning or operational documents and information from the risk assessment, if the expected vulnerabilities in the information system and resulting expected residual risk to the agency appear to be correct and reasonable. Based on the results of this independent review and analysis, the certification agent and authorizing official or designated representative may recommend changes to: (i) the security controls; (ii) the expected vulnerabilities; or (iii) other sections in the security plan, as appropriate.

REFERENCE: [NIST Special Publications 800-18 or equivalent]

SECURITY PLAN UPDATE

SUBTASK 3.2: Update the security plan based on the results of the independent analysis and recommendations of the certification agent and the authorizing official or designated representative.

RESPONSIBILITY: [Information System Owner, Information System Security Officer]

ADVISORY NOTE: The system information owner reviews the changes recommended by the certification agent and authorizing official or designated representative and consults with other agency representatives (e.g., information owner, information system security officer, or user representative), as appropriate, prior to making any final modifications to the security plan. The modifications to the security plan may include any of the areas described in the first security certification and accreditation task (e.g., adding or eliminating security controls, changing the expected vulnerabilities, or modifying the expected residual risk).

REFERENCE: [NIST Special Publication 800-18 or equivalent]

SECURITY PLAN ACCEPTANCE

SUBTASK 3.3: Review the security plan to determine if the expected residual risk to agency operations (including mission, functions, image, or reputation) or agency assets is acceptable.

RESPONSIBILITY: [Authorizing Official or Designated Representative]

ADVISORY NOTE: If the expected residual risk in the security plan is deemed unacceptable, the authorizing official or designated representative sends the plan back to the information system owner for appropriate action. If the expected residual risk in the security plan is deemed acceptable, the authorizing official or designated representative accepts the plan. The acceptance of the security plan represents an important milestone in the security certification and accreditation of the information system. The authorizing official or designated representative, by accepting the security plan, is agreeing to move ahead to the next phase of the security certification and accreditation process (i.e., the actual testing and evaluation of security controls) and is also approving the level of effort and resources required to successfully complete the associated security certification and accreditation activities.

REFERENCE: [NIST Special Publication 800-30 or equivalent]

Key Milestone:

The following questions must be answered before proceeding to the next phase—Security Certification.

- **Is the FIPS Publication 199 risk level described in the security plan correct?**
- **Does the execution plan properly identify the resources required to successfully complete the security certification and accreditation activities?**
- **Does the expected residual risk described in the security plan appear to be correct?**
- **Having decided that the expected residual risk appears to be correct, would the risk be acceptable?**

3.2 SECURITY CERTIFICATION PHASE

The Security Certification Phase consists of two tasks: (i) security control verification; and (ii) security certification documentation. The purpose of this phase is to ensure that the actual vulnerabilities in the information system are determined through independent evaluation of the security controls and that recommended corrective actions are provided to the information system owner and authorizing official. Upon successful completion of this phase, the authorizing official will have the information needed from the security certification to determine the actual residual risk to agency operations and assets—and thus, will be able to render an appropriate security accreditation decision for the information system.

TASK 4: SECURITY CONTROL VERIFICATION

The objective of this task is to: (i) prepare for the evaluation of the security controls in the information system; (ii) evaluate the security controls; and (iii) document the results of the evaluation. Preparation for security evaluation involves gathering appropriate planning and supporting material, system requirements and design documentation, security control implementation evidence, and assessment results from previous security evaluations, security reviews, or audits. Preparation also involves developing specific techniques and procedures to evaluate the security controls in the information system. The certification agent, at the completion of this task, will be able to describe the actual vulnerabilities in the information system and be in a position to offer informed recommendations to the authorizing official.

DOCUMENTATION AND SUPPORTING MATERIALS

SUBTASK 4.1: Assemble any documentation and supporting materials necessary for the evaluation of the security controls in the information system.

RESPONSIBILITY: [Information System Owner, Certification Agent]

ADVISORY NOTE: The information system owner should assist the certification agent in gathering all relevant documents and supporting materials from the agency that will be required during the evaluation of the security controls. Descriptive information about the information system is typically documented in the system identification section of the security plan or in some cases, included as attachments to the plan. System identification information can also be provided by referencing appropriate documents. Supporting materials such as procedures, reports, logs, and records showing evidence of security control implementation should be identified as well.

REFERENCE: [Documents and supporting materials included or referenced in the security plan]

REUSE OF EVALUATION RESULTS

SUBTASK 4.2: Assemble and review the findings, results, evidence, and documentation from previous assessments (e.g., developmental/operational security testing and evaluation, type certifications, site certifications, audits, security reviews, self-assessments) of the security controls in the information system for use during the security certification and accreditation process.

RESPONSIBILITY: [Information System Owner, Certification Agent]

ADVISORY NOTE: Evaluating the security controls in an information system can be a very costly and time-consuming process. In order to make the security certification and accreditation process as timely and cost effective as possible, the reuse of previous evaluation results, when reasonable and appropriate, is strongly recommended. For example, a recent audit of an information system by an independent auditor may have produced important information about the effectiveness of selected security controls. Another opportunity to reuse previous evaluation results comes from programs that independently test and evaluate the security features of commercial information technology products. And finally, if prior evaluation results from the system developer are available, the certification agent, under appropriate circumstances may incorporate those evaluation results into the security certification (e.g., repeating only a portion of the developer's evaluation to verify the results and subsequently relying on the remainder of the results without the necessity for reevaluation). Certification agents should maximize the use of previous evaluation results in determining the effectiveness of security controls in an information system.

REFERENCE: [Independent audits, security reviews, test and evaluation reports, self-assessments]

TECHNIQUES AND PROCEDURES

SUBTASK 4.3: Select, or develop when needed, appropriate techniques and procedures to evaluate the management, operational, and technical security controls in the information system.

RESPONSIBILITY: [Certification Agent]

ADVISORY NOTE: In lieu of developing unique or specialized techniques and procedures to evaluate the security controls in the information system, certification agents should consult NIST Special Publication 800-53A, which provides standardized evaluation techniques and procedures for verifying the effectiveness of security controls listed in NIST Special Publication 800-53. These evaluation techniques and procedures can be supplemented by the agency, if needed. Evaluation techniques and procedures may need to be created for those security controls employed by the agency that are not contained in NIST Special Publication 800-53. Additionally, evaluation techniques and procedures may need to be tailored in some instances, for specific system implementations.

REFERENCE: [NIST Special Publication 800-53A or equivalent]

SECURITY EVALUATION

SUBTASK 4.4: Evaluate the management, operational, and technical security controls in the information system using techniques and procedures selected or developed in Subtask 4.3, to determine the effectiveness of those controls in a particular environment of operation

and the remaining vulnerabilities in the system after the implementation of such controls.

RESPONSIBILITY: [Certification Agent]

ADVISORY NOTE: Security evaluation provides important insights into the effectiveness of the security controls in the information system. Certain security controls may not have been appropriately implemented in the system, while others may be deemed to be less than effective. After the security evaluation is completed, the certification agent will have determined the state of the security controls and actual vulnerabilities in the information system. The results of the security evaluation (including the confirmed vulnerabilities in the information system) are documented in the security test and evaluation report.

REFERENCE: [NIST Special Publication 800-53A or equivalent]

SECURITY TEST AND EVALUATION REPORT

SUBTASK 4.5: Prepare the final security test and evaluation report.

RESPONSIBILITY: [Certification Agent]

ADVISORY NOTE: The security test and evaluation report contains: (i) the results of the security evaluation (i.e., the determination of security control effectiveness); (ii) a description of the confirmed vulnerabilities in the information system; and (iii) recommendations for corrective actions that could be taken to reduce or eliminate the vulnerabilities. The security test and evaluation report is part of the final security certification package along with the updated security plan and plan of action and milestones. The security test and evaluation report is the certification agent's statement regarding the security status of the information system.

REFERENCE: [NIST Special Publication 800-53A or equivalent]

TASK 5: SECURITY CERTIFICATION DOCUMENTATION

The objective of this task is to: (i) provide the certification agent findings and recommendations to the information system owner; (ii) update the security plan as needed; and (iii) assemble the final security certification package. The system owner has an opportunity to reduce or eliminate vulnerabilities in the information system prior to the assembly and compilation of the final security certification package and submission to the authorizing official. This is accomplished by implementing corrective actions recommended by the certification agent. The certification agent should evaluate any security controls modified, enhanced, or added during this process to ensure the confirmed vulnerabilities remain accurate. The completion of this task will conclude the Security Certification Phase.

CERTIFICATION AGENT FINDINGS AND RECOMMENDATIONS

SUBTASK 5.1: Provide the information system owner with a security test and evaluation report.

RESPONSIBILITY: [Certification Agent]

ADVISORY NOTE: The information system owner relies on the security expertise and the technical judgment of the certification agent to: (i) assess the effectiveness of the security controls in the information system; (ii) determine the actual vulnerabilities in the system; and (iii) provide specific recommendations on how to strengthen, fix, or add security controls to reduce or eliminate identified vulnerabilities. The system owner may choose to act on selected recommendations of the certification agent be-

fore the security certification package is finalized if there are specific opportunities to reduce or eliminate vulnerabilities in the information system prior to the final security accreditation decision by the authorizing official. The certification agent evaluates any changes made to the security controls in response to corrective actions by the system owner and updates the recommendations for corrective actions and information system vulnerabilities, as appropriate.

REFERENCE: [NIST Special Publication 800-30 or equivalent]

SECURITY PLAN UPDATE

SUBTASK 5.2: Update the security plan based on the results of the security evaluation and any modifications to the security controls in the information system.

RESPONSIBILITY: [Information System Owner, Information System Security Officer]

ADVISORY NOTE: The security plan should reflect the actual state of the security controls after the security evaluation and any modifications by the information system owner in addressing the recommendations for corrective actions from the certification agent. The plan, at the completion of the Security Certification Phase, should contain: (i) an accurate list and description of security controls; and (ii) a description of the actual vulnerabilities in the information system resulting from the ineffectiveness or absence of security controls (i.e., controls *not* implemented). The actual vulnerabilities replace the expected vulnerabilities described in the original security plan.

REFERENCES: [NIST Special Publications 800-18 or equivalent]

SECURITY CERTIFICATION PACKAGE ASSEMBLY

SUBTASK 5.3: Assemble the final security certification package.

RESPONSIBILITY: [Information System Owner, Information System Security Officer, Certification Agent]

ADVISORY NOTE: The information system owner is responsible for the assembly and compilation of the final security certification package with inputs from the information system security officer and the certification agent. The security certification package contains the following information: (i) the security test and evaluation report from the certification agent providing the results of the independent evaluation of the security controls in the information system, the confirmed vulnerabilities in the system, and recommendations for corrective actions; (ii) the action plan from the system owner (including milestones and costs) indicating corrective actions taken or planned to reduce or eliminate the vulnerabilities in the information system; and (iii) the updated security plan. The certification agent's input to the final security certification package provides an unbiased and independent view of the effectiveness of the security controls in the information system. The information system owner may also wish to consult with other key agency participants (e.g., the user representative) prior to submitting the final security certification package to the authorizing official or designated representative. The authorizing official or designated representative will use this information during the Security Accreditation Phase to determine the actual residual risk to agency operations (including mission, functions, image, or reputation) or agency assets. The contents of the security certification package should be protected appropriately in accordance with agency policy.

REFERENCE: [OMB Circular A-130]

Key Milestone:

The following questions must be answered before proceeding to the next phase—Security Accreditation.

- **What are the actual vulnerabilities in the information system?**
- **What specific corrective actions have been taken or are planned to reduce or eliminate vulnerabilities in the information system?**

3.3 SECURITY ACCREDITATION PHASE

The Security Accreditation Phase consists of two tasks: (i) security accreditation decision; and (ii) security accreditation documentation. The purpose of this phase is to ensure that the actual residual risk to agency operations (including mission, functions, image, or reputation) or agency assets is acceptable to the authorizing official and that the acceptability of that risk forms the basis of the security accreditation decision. Upon successful completion of this phase, the information system owner will have: (i) full authorization to operate the information system; (ii) an interim approval to operate the information system under specific terms and conditions; or (iii) denial of authorization to operate the information system.

TASK 6: SECURITY ACCREDITATION DECISION

The objective of this task is to: (i) determine the actual residual risk to the agency's operations or assets; (ii) determine if the actual residual risk is acceptable; and (iii) prepare the final security accreditation package. The authorizing official or designated representative, working with information from the information system owner, information system security officer, and certification agent produced during the previous phase, has independent confirmation of the actual vulnerabilities in the information system and a list of planned or completed corrective actions to reduce or eliminate those vulnerabilities. It is this information that is used to determine the final residual risk to the agency and the acceptability of that risk.

RESIDUAL RISK DETERMINATION (ACTUAL)

SUBTASK 6.1: Determine the actual residual risk to agency operations (including mission, functions, image, or reputation) or agency assets based on the confirmed vulnerabilities in the information system and any planned or completed corrective actions to reduce or eliminate those vulnerabilities.

RESPONSIBILITY: [Authorizing Official or Designated Representative]

ADVISORY NOTE: The authorizing official or designated representative receives the final security certification package from the information system owner. The actual vulnerabilities in the information system confirmed by the certification agent should be assessed to determine how those particular vulnerabilities translate into actual risk to agency operations or agency assets. The authorizing official or designated representative should judge which information system vulnerabilities are of greatest concern to the agency and which vulnerabilities can be tolerated without creating unreasonable risk to agency operations (including mission, functions, image, or reputation) or agency assets. The action plan to reduce or eliminate vulnerabilities (including milestones and estimated costs) submitted by the information system owner should also be considered in determining the risk to the agency. The authorizing official or designated representative may consult the information system owner, certification agent, or other agency officials before making the final risk determination.

REFERENCE: [NIST Special Publication 800-30 or equivalent]

RESIDUAL RISK ACCEPTABILITY

SUBTASK 6.2: Determine if the actual residual risk to agency operations or agency assets is acceptable and prepare the final security accreditation package.

RESPONSIBILITY: [Authorizing Official]

ADVISORY NOTE: The authorizing official should consider many factors when deciding if the residual risk to agency operations or agency assets is acceptable. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable security accreditation decision. The authorizing official renders an accreditation decision for the information system after reviewing all of the relevant information and, where appropriate, consulting with key agency officials.

- If, after assessing the results of the security certification, the actual residual risk to agency operations (including mission, functions, image, or reputation) or agency assets is deemed acceptable to the authorizing official, a full authorization to operate is issued. The information system is accredited without any restrictions or limitations on its operation.
- If, after assessing the results of the security certification, the actual residual risk to agency operations or agency assets is not deemed fully acceptable to the authorizing official but there is an important mission-related need to place the information system into operation, an interim approval to operate may be issued. The interim approval to operate is a limited authorization under specific terms and conditions including corrective actions to be taken by the information system owner and a required timeframe for completion of those actions. A detailed plan of action and milestones should be submitted by the information system owner and approved by the authorizing official prior to the interim approval to operate taking effect. The information system is *not* accredited during the period of limited authorization to operate.
- If, after assessing the results of the security certification, the actual residual risk to agency operations or agency assets is deemed unacceptable to the authorizing official, the information system is not authorized for operation, and thus, is *not* accredited.

The final security accreditation package is prepared by the authorizing official's designated representative or administrative staff. The format and content of the security accreditation package is at the discretion of the agency but typically consists of a security accreditation decision letter signed by the authorizing official. The letter includes the security accreditation decision, the rationale for the decision, the terms and conditions for information system operation including required corrective actions, if appropriate, and any attachments that the authorizing official wishes to provide to the information system owner (e.g., the security certification package). The contents of the security accreditation package should be protected appropriately in accordance with agency policy.

REFERENCE: [OMB Circular A-130]

TASK 7: SECURITY ACCREDITATION DOCUMENTATION

The objective of this task is to: (i) transmit the final security accreditation package to the appropriate individuals and organizations; and (ii) update the security plan with the latest information

from the accreditation decision. The completion of this task will conclude the Security Accreditation Phase of the security certification and accreditation process.

SECURITY ACCREDITATION PACKAGE TRANSMISSION

SUBTASK 7.1: Provide copies of the final security accreditation package to the information system owner and any other agency officials having an interest (i.e., need to know) in the security of the information system.

RESPONSIBILITY: [Authorizing Official or Designated Representative]

ADVISORY NOTE: The security accreditation package contains important documents. The package should be safeguarded appropriately and stored, whenever possible, in a centralized agency filing system to ensure accessibility. The security accreditation package should also be readily available to auditors and oversight agencies upon request.

REFERENCE: [OMB Circular A-130]

SECURITY PLAN UPDATE

SUBTASK 7.2: Update the security plan based on the final determination of actual residual risk to agency operations or agency assets.

RESPONSIBILITY: [Information System Owner, Information System Security Officer]

ADVISORY NOTE: The security plan should be updated to reflect any changes in the information system resulting from the Security Accreditation Phase. Any conditions set forth in the accreditation decision should also be noted in the plan. It is expected that the changes to the security plan at this phase in the security certification and accreditation process would be minimal.

REFERENCES: [NIST Special Publications 800-18 or equivalent]

Key Milestone:

The following questions must be answered before proceeding to the next phase—Continuous Monitoring.

- **How do the actual vulnerabilities in the information system translate into actual residual risk to agency operations or agency assets?**
- **Is the actual residual risk acceptable?**

3.4 CONTINOUS MONITORING PHASE

The Continuous Monitoring Phase consists of three tasks: (i) configuration management and control; (ii) ongoing security control verification; 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 or designated representative when changes occur that may impact on the security of the system. The activities in this phase continue until the need for security reaccreditation occurs, either because of specific changes to the information system (event-driven) or because of federal or agency policies requiring reauthorization of the system at a specified timeframe.

TASK 8: CONFIGURATION MANAGEMENT AND CONTROL

The objectives of this task are to: (i) document the proposed or actual changes to the information system; and (ii) determine the impact of those proposed or actual changes on the security of the system. Information systems will typically be in a constant state of migration with upgrades to hardware, software, or firmware and possible modifications to the surrounding environment where the system resides. Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation.

DOCUMENTATION OF INFORMATION SYSTEM CHANGES

SUBTASK 8.1: Using established agency configuration management and configuration control procedures, document proposed or actual changes to the information system (including hardware, software, firmware, and surrounding environment).

RESPONSIBILITY: [Information System Owner, Information System Security Officer, Cognizant Configuration Control Board]

ADVISORY NOTE: An orderly and disciplined approach to managing, controlling, and documenting changes to an information system is critical to the ongoing assessment of the security controls that protect the system. It is important to record any relevant information about the specific proposed or actual changes to the hardware, firmware, or software such as version or release numbers, descriptions of new or modified features or capabilities, and security implementation guidance, if available. It is also important to record any changes to the surrounding environment of the information system such as modifications to the physical plant where the system resides. The information system owner and information system security officer should use this information in assessing the potential security impact of the proposed or actual changes to the information system. Significant changes to the information system should not be undertaken prior to assessing the security impact of such changes.

REFERENCE: [Agency policies/procedures on configuration management and control]

SECURITY IMPACT ANALYSIS

SUBTASK 8.2: Analyze the proposed or actual changes to the information system (including hardware, software, firmware, and surrounding environment) to determine the security impact of such changes.

RESPONSIBILITY: [Information System Owner, Information System Security Officer]

ADVISORY NOTE: Changes to the information system may affect the security controls currently in place, produce new vulnerabilities in the system, or generate requirements for new security controls that were not needed previously. The degree or level of rigor applied to the security impact analysis is at the discretion of the agency but should be guided by the risk level of the information system (in accordance with FIPS Publication 199). If the results of the security impact analysis indicate that the proposed or actual changes to the information system will affect or have affected the security of the information system, corrective actions should be initiated and a plan of action and milestones developed. The information system owner or information system security officer may wish to consult with the user representative or other agency officials prior to implementing any security-related changes to the information system. Conducting a security impact analysis is part of the ongoing assessment of risk within the agency.

REFERENCE: [NIST Special Publication 800-30 or equivalent]

TASK 9: ONGOING SECURITY CONTROL VERIFICATION

The objective of this task is to: (i) select an appropriate set of security controls in the information system to be monitored; and (ii) evaluate the effectiveness of the selected controls using verification techniques and procedures selected by the agency. The ongoing verification of security control effectiveness helps to identify potential security-related problems in the information system that are not identified during the security impact analysis conducted as part of the configuration management and control process.

SECURITY CONTROL SELECTION

SUBTASK 9.1: Using agency-defined selection criteria, identify a subset of the security controls in the information system that should be evaluated to determine the continued effectiveness of those controls in providing appropriate protection for the system.

RESPONSIBILITY: [Information System Owner, Information System Security Officer]

ADVISORY NOTE: The criteria established by the agency for selecting which security controls will be monitored should reflect the agency's priorities and importance of the information system to the agency. For example, certain security controls may be considered more critical than other controls because of the potential impact on the information system if those controls were subverted or found to be ineffective. The risk level of the information system (in accordance with FIPS Publication 199) should also be considered in any decisions about security control monitoring. The security controls being monitored should be reviewed over time to ensure that as many controls as possible in the information system are evaluated to determine continued effectiveness. The authorizing official or designated representative and information system owner (in consultation with the information system security officer) should agree on the subset of the security controls in the information system that should be monitored on an ongoing basis as well as the frequency of such monitoring activity.

REFERENCES: [FISMA, OMB Circular A-130, NIST Special Publications 800-53]

SECURITY CONTROL MONITORING

SUBTASK 9.2: Evaluate the agreed upon set of security controls in the information system to determine the continued effectiveness of those controls in providing appropriate protection for the system.

RESPONSIBILITY: [Information System Owner, Information System Security Officer]

ADVISORY NOTE: The ongoing monitoring of security control effectiveness can be accomplished in a variety of ways including security reviews, self-assessments, security testing and evaluation, or audits. The techniques and procedures employed to evaluate security control effectiveness during the monitoring process are at the discretion of the agency. In lieu of developing unique or specialized techniques and procedures to evaluate the security controls in the information system, system owners or information system security officers should consult NIST Special Publication 800-53A, which provides standardized evaluation techniques and procedures for the security controls listed in NIST Special Publication 800-53. The monitoring process should be documented and available for review by the authorizing official or designated representative, upon request. If the results of the security evaluation indicate that selected controls are less than effective in their application and are affecting the security of the information system, corrective actions should be initiated and a plan of action and milestones developed.

REFERENCES: [FISMA, OMB Circular A-130, NIST Special Publications 800-53A, 800-26]

TASK 10: STATUS REPORTING AND DOCUMENTATION

The objective of this task is to: (i) update the security plan to reflect the most recent proposed or actual changes to the information system and any identified or potential security impacts; and (ii) report the proposed or actual changes and identified or potential security impacts to the authorizing official or designated representative. The information in the status reports should be used to determine the need for security reaccreditation.

SECURITY PLAN UPDATE

SUBTASK 10.1: Update the security plan based on the documented changes to the information system (including hardware, software, firmware, and surrounding environment) and the results of the ongoing process to monitor the effectiveness of the security controls in the information system.

RESPONSIBILITY: [Information System Owner, Information System Security Officer]

ADVISORY NOTE: The security plan should contain the most up-to-date information about the information system. Changes to the information system should be reflected in the security plan. The frequency of security plan updates is at the discretion of the agency. The updates should occur at appropriate intervals to capture significant changes to the information system, but not so frequently as to generate unnecessary paperwork. The risk level of the information system (in accordance with FIPS Publication 199) should also be considered in any decisions about frequency of security plan updates. The authorizing official, information system owner, information system security officer, and certification agent will be using the security plan to guide any future security certification and accreditation activities, when required.

REFERENCE: [NIST Special Publication 800-18 or equivalent]

STATUS REPORTING

SUBTASK 10.2: Report the security status of the information system to the authorizing official or designated representative.

RESPONSIBILITY: [Information System Owner]

ADVISORY NOTE: The security status report should describe the continuous monitoring activities employed by the agency and include a plan of action and milestones. The plan of action and milestones address vulnerabilities in the information system discovered during the security impact analysis or security control monitoring and how the information system owner intends to deal with those vulnerabilities (i.e., reduce, eliminate, or accept the vulnerabilities). The frequency of security status reports is at the discretion of the agency. The status reports should occur at appropriate intervals to transmit significant security-related information about the system, but not so frequently as to generate unnecessary paperwork. The risk level of the information system (in accordance with FIPS Publication 199) should also be considered in any decisions about frequency of security status reporting. The authorizing official or designated representative should use the security status reports to determine if a security reaccreditation is necessary. The authorizing official or designated representative should notify the information system owner if there is a decision to require a security reaccreditation of the information system. A decision to reaccredit the information system should begin, as in the original security accreditation, with the Initiation

Phase. Depending on the magnitude of the changes to the information system and the extent of the security controls affected, the resources required for the security reaccreditation may be substantially less than the original security accreditation.

REFERENCE: [FISMA, OMB Circular A-130]

Key Milestone:

The following questions must be answered before reinitiating the security certification and accreditation process for the information system—

- **Have any changes to the information system affected the current, documented vulnerabilities in the system?**
- **If so, has the actual residual risk to agency operations or assets been affected?**

OR

- **Has a specified time period passed requiring the information system to be reauthorized in accordance with federal or agency policy?**

ANNEX A

REFERENCES

LAWS, POLICIES, REGULATIONS, STANDARDS, AND SPECIAL PUBLICATIONS

1. Privacy Act of 1974, (Public Law 93-579), September 1975.
2. Paperwork Reduction Act of 1995, (Public Law 104-13), May 1995.
3. Information Technology Management Reform Act of 1996, (Public Law 104-106), August 1996.
4. Federal Information Security Management Act of 2002, (Public Law 107-347), December 2002.
5. OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Resources*, February 1996.
6. Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, (Initial public draft), May 2003.
7. NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.
8. NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, January 2002.
9. NIST Special Publication 800-53, *Security Controls for Federal Information Systems*, (Initial public draft projected for publication, Summer 2003).
10. NIST Special Publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems*, (Initial public draft projected for publication, Winter 2003-04).
11. NIST Special Publication 800-60, *Guide for Mapping Information and Information Types to Security Objectives and Risk Levels*, (Initial public draft projected for publication, Fall 2003).

ANNEX B

GLOSSARY

COMMON TERMS ASSOCIATED WITH SECURITY CERTIFICATION AND ACCREDITATION

The terms and definitions in this special publication and have been obtained from Congressional legislation, Executive Orders, OMB policies, and commonly accepted glossaries of security terminology.

Acceptable Risk	A concern that is acceptable to responsible management, due to the cost and magnitude of implementing security controls.
Adequate Security	Security commensurate with risk, including the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Agency	See Executive Agency.
Application	The use of information resources (information and information technology) to satisfy a specific set of user requirements.
Authenticity	The property of being genuine and able to be verified and be trusted; assurance of the validity of a transmission, message, or originator within an information system. See authentication.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authorize Processing	See Security Accreditation.
Authorizing Official	The senior management official or executive with the authority to approve the operation of an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Also known as Designated Approving Authority or Designated Accrediting Authority.
Authorizing Official Designated Representative	An agency staff member selected by the authorizing official to act on his or her behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of the information system.
Availability [44 U.S.C., SEC. 3542]	Ensuring timely and reliable access to and use of information.

Certification Agent	The individual responsible for conducting a comprehensive evaluation of the management, operational, and technical security controls in an information system to determine: (i) the effectiveness of the controls in a particular environment of operation; and (ii) the remaining vulnerabilities in the system after the implementation of such controls.
Confidentiality [44 U.S.C., SEC. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Countermeasures	Synonymous with security controls and safeguards.
Designated Accrediting Authority	See Authorizing Official.
Executive Agency [41 U.S.C., SEC. 403]	An executive department specified in 5 U.S.C., Section 101; a military department specified in 5 U.S.C., Section 102; an independent establishment as defined in 5 U.S.C., Section 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.
Executive Departments [5 U.S.C., SEC.101]	Department of State, Department of the Treasury, Department of Defense, Department of Justice, Department of the Interior, Department of Agriculture, Department of Commerce, Department of Labor, Department of Health and Human Services, Department of Housing and Urban Development, Department of Transportation, Department of Energy, Department of Education, Department of Veterans Affairs, Department of Homeland Security.
Federal Information System [40 U.S.C., SEC. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
General Support System	An interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people, and provides support for a variety of users and applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.
Information Resources [44 U.S.C., SEC. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security [44 U.S.C., SEC. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information System [44 U.S.C., SEC. 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Owner	The agency official that represents the interests of the user community throughout the life cycle of the information system.
Information System Security Officer	The principal staff advisor to the information system owner on all matters (technical and otherwise) involving the security of the information system.
Information Technology [40 U.S.C., SEC. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. Equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Major Application	An application that requires special attention to security due to risk, including magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.
Major Information System	An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.
Military Departments [5 U.S.C., SEC. 102]	Department of the Army, Department of the Navy, and Department of the Air Force.

National Security Information	Information that has been determined pursuant to Executive Order 12958 or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.
National Security System [44 U.S.C., SEC. 3542]	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or, (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Non-repudiation	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later legitimately deny having processed, stored, or transmitted the information.
Residual Risk	The portion of risk remaining after the application of appropriate security controls in the information system.
Risk	A combination of: (i) the likelihood that a particular vulnerability in an agency information system will be either intentionally or unintentionally exploited by a particular threat resulting in a loss of confidentiality, integrity, or availability; and (ii) the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability will have on agency operations (including mission, functions, image, or reputation), agency assets, or individuals (including privacy) should the exploitation occur.
Risk Assessment	A key component of risk management that brings together important information for agency officials with regard to the protection of information and information systems including: (i) the identification of threats and vulnerabilities; (ii) the identification and analysis of security controls; (iii) the analysis of impact or magnitude of harm that a loss of confidentiality, integrity, or availability would have on agency operations (including mission, functions, image, or reputation), agency assets, or individuals; (iv) the likelihood of threat exploitation of vulnerabilities; and (v) determination of risk.

Risk Management	The process of identifying, controlling, and mitigating risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system or multiple information systems. It includes: risk assessment, cost benefit analysis, and the selection, implementation, testing and evaluation of security controls.
Safeguards	Synonymous with security controls and countermeasures.
Security	See Information Security.
Security Accreditation	The official management decision to authorize operation of an information system. This authorization, given by a senior agency official, is applicable to a particular environment of operation, and explicitly accepts the level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, remaining after the implementation of an agreed upon set of security controls.
Security Certification	A comprehensive evaluation of the management, operational, and technical security controls in an information system. This evaluation, made in support of the security accreditation process, determines the effectiveness of these security controls in a particular environment of operation and the remaining vulnerabilities in the information system after the implementation of such controls.
Security Controls	The management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information.
Security Plan	Formal document that provides an overview of the security requirements of the information system and describes the security controls in place or planned for meeting those requirements.
Security Control Robustness	The strength of a security control and the assurance that the control is effective in its operation.
Subsystem	A major subdivision or component of an information system consisting of hardware, software, or firmware that performs a specific function.
Threat	Any circumstance or event with the potential to intentionally or unintentionally exploit a specific vulnerability in an information system resulting in a loss of confidentiality, integrity, or availability.

User Representative	The individual that represents the operational interests of the user community and serves as the liaison for that community throughout the life cycle of the information system.
Verification	The process used by an independent certification agent to confirm or establish by testing, evaluation, examination, investigation or competent evidence.
Vulnerability	A flaw or weakness in the design or implementation of an information system (including the security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely effect an agency's operations (including mission, functions, image, or reputation), an agency's assets, or individuals (including privacy) through a loss of confidentiality, integrity, or availability.

ANNEX C

ACRONYMS

SHORTHAND NOTATIONS FOR CERTIFICATION AND ACCREDITATION-RELATED TERMS

COTS	Commercial Off The Shelf
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
MOA	Memorandums of Agreement
MOU	Memorandums of Understanding
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
U.S.C.	United States Code

ANNEX D

SUMMARY OF ROLES AND RESPONSIBILITIES

MAJOR RESPONSIBILITIES AND ACTIVITIES FOR KEY PARTICIPANTS

ROLE	RESPONSIBILITIES
AUTHORIZING OFFICIAL OR DESIGNATED REPRESENTATIVE	• Reviews and approves the security plan for the information system • Determines residual risk to agency operations or assets based on information generated during the security certification • Makes security accreditation decision and signs associated accreditation decision letter for accreditation package (authorizing official only) • Reviews security status reports from continuous monitoring operations • Initiates security reaccreditation actions
INFORMATION SYSTEM OWNER	• Represents the interests of the user community • Prepares security plan and conducts risk assessment • Informs agency officials of the need for security certification and accreditation of the information system; ensures appropriate resources are available • Provides the necessary system-related documentation to the certification agent • Prepares plan of action (and milestones) to reduce or eliminate vulnerabilities in the information system • Assembles final security certification package; submits to authorizing official
INFORMATION SYSTEM SECURITY OFFICER	• Serves as principal staff advisor to the system owner on all matters involving the security of the information system • Manages the security aspects of the information system and, in some cases, oversees the day-to-day security operations of the system • Assists the system owner in developing and enforcing security policies for the information system • Assists the system owner in assembling the security certification package • Assists the system owner in managing and controlling changes to the information system as well as assessing the security impacts of those changes
CERTIFICATION AGENT	• Provides an independent assessment of the security plan • Evaluates the security controls in the information system to determine: (i) the effectiveness of those controls in a particular environment of operation; and (ii) the vulnerabilities in the system after the implementation of such controls • Provides recommended corrective actions to reduce or eliminate vulnerabilities in the information system
USER REPRESENTATIVE	• Represents the operational interests and mission needs of the user community • Identifies mission and operational requirements • Serves as the liaison for user community throughout the life cycle of the information system • Assists in the security certification and accreditation process, when needed

FIGURE D.1 SUMMARY OF ROLES AND RESPONSIBILITIES

ANNEX E

SAMPLE CERTIFICATION AND ACCREDITATION LETTERS

FULL AUTHORIZATION, INTERIM APPROVAL TO OPERATE, AND DENIAL OF AUTHORIZATION

Security Certification Letter

To: Authorizing Official Date:
From: Information System Owner

Subject: Security Certification of [INFORMATION SYSTEM]

A security certification of the [INFORMATION SYSTEM] and its constituent system-level components (if applicable) located at [LOCATION] has been conducted in accordance with Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, and the [AGENCY] policy on security accreditation. The attached security certification package contains the following items: (i) the current security plan for the information system; (ii) the security test and evaluation report; and (iii) the plan of action and milestones.

The security controls listed in the security plan for the information system have been evaluated by [CERTIFICATION AGENT] using the verification techniques and the procedures described in the security test and evaluation report to determine if those controls are effective in their application. Based on the results of the security test and evaluation activities, the actual vulnerabilities in the information system have been identified and a list of recommended corrective actions prepared. The plan of action and milestones describes the corrective measures that have been implemented or planned to reduce or eliminate the stated vulnerabilities in the information system.

Signature:

Title:

Enclosures: as

Security Accreditation Decision Letter

(Full Authorization to Operate)

To: Information System Owner Date:
From: Authorizing Official

Subject: Security Accreditation Decision for [INFORMATION SYSTEM]

A security certification of the [INFORMATION SYSTEM] and its constituent system-level components (if applicable) located at [LOCATION] has been conducted in accordance with Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, and the [AGENCY] policy on security accreditation. After reviewing the results of the security certification and the supporting evidence provided in the associated security certification package (including the current security plan for the information system, the security test and evaluation report, and the plan of action and milestones), I have determined that the confirmed vulnerabilities in the information system result in a residual risk to the operations/assets of this agency that is fully acceptable. Accordingly, I am issuing a full authorization to operate the information system in its existing operating environment; the system is accredited without any significant restrictions or limitations. This security accreditation is my formal declaration that appropriate security controls have been implemented in the information system and that a satisfactory level of security is present in the system.

The security accreditation of the information system will remain in effect as long as: (i) the required security status reports for the system are submitted to this office in accordance with NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*; (ii) the confirmed vulnerabilities reported during the continuous monitoring process do not result in additional risk to the agency's operations/assets which is deemed unacceptable; and (iii) the system has not exceeded the maximum allowable time period between security authorizations (in accordance with federal or agency policy).

The information system owner should retain a copy of this letter with all supporting security certification and accreditation documentation as a permanent record.

Signature:

Title:

Enclosures: as

Security Accreditation Decision Letter

(Interim Approval to Operate)

To: Information System Owner Date:
From: Authorizing Official

Subject: Security Accreditation Decision for [INFORMATION SYSTEM]

A security certification of the [INFORMATION SYSTEM] and its constituent system-level components (if applicable) located at [LOCATION] has been conducted in accordance with Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, and the [AGENCY] policy on security accreditation. After reviewing the results of the security certification and the supporting evidence provided in the associated security certification package (including the current security plan for the information system, the security test and evaluation report, and the plan of action and milestones), I have determined that the confirmed vulnerabilities in the information system result in a residual risk to the operations/assets of this agency that is not fully acceptable. However, I have also determined that there is an overarching need to place the information system into operation or continue its operation due to mission necessity. Accordingly, I am issuing an interim approval to operate the information system in its existing operating environment. An interim approval is a limited authorization to operate the information system under specific terms and conditions and acknowledges greater risk to the agency's operations and assets for a limited period of time. The terms and conditions of this limited authorization are described in Attachment A. The information system is *not* considered accredited during the period of limited authorization to operate. A disciplined and structured process must be established by the agency to monitor the effectiveness of the security controls in the information system during the period of limited authorization. Monitoring activities should focus on the specific areas of concern identified during the security certification. Significant changes in the security state of the information system during the period of limited authorization should be reported immediately.

This interim approval to operate the information system is valid for [TIME PERIOD]. The limited authorization will remain in effect during that time period as long as: (i) the required security status reports for the system are submitted to this office in accordance with NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*; and (ii) the confirmed vulnerabilities reported during the continuous monitoring process do not result in additional risk to the agency's operations/assets which is deemed unacceptable; and (iii) continued progress is being made on reducing or eliminating vulnerabilities in the information system in accordance with the plan of action and milestones. At the end of the period of limited authorization, the information system must be either fully authorized to operate or the authorization for further operation will be denied. Renewals or extensions to this interim approval to operate will be granted only under the most extreme or extenuating of circumstances.

The information system owner should retain a copy of this letter with all supporting security certification and accreditation documentation as a permanent record.

Signature:

Title:

Enclosures: as

Security Accreditation Decision Letter

(Denial of Authorization to Operate)

To: Information System Owner Date:
From: Authorizing Official

Subject: Security Accreditation Decision for [INFORMATION SYSTEM]

A security certification of the [INFORMATION SYSTEM] and its constituent system-level components (if applicable) located at [LOCATION] has been conducted in accordance with Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, and the [AGENCY] policy on security accreditation. After reviewing the results of the security certification and the supporting evidence provided in the associated security certification package (including the current security plan for the information system, the security test and evaluation report, and the plan of action and milestones), I have determined that the confirmed vulnerabilities in the information system result in a residual risk to the operations/assets of this agency that is unacceptable. Accordingly, I am issuing a denial of authorization to operate the information system in its existing operating environment. The information system is *not* accredited and may not be placed into operation—or, if the system is currently in operation, all activity must be halted. Failure to receive an authorization to operate the information system indicates that there are major deficiencies in the security controls in the system and that a satisfactory level of security is not present in the system.

The information system owner should revise the plan of action and milestones and ensure that proactive measures are taken to correct the security deficiencies in the information system. The security certification should be repeated at the earliest opportunity to determine the effectiveness of the security controls in the information system after the reduction or elimination of identified vulnerabilities.

The information system owner should retain a copy of this letter with all supporting security certification and accreditation documentation as a permanent record.

Signature:

Title:

Enclosures: as

ANNEX F

INFORMATION SECURITY PROGRAM ACTIVITIES

INTEGRATING THE SECURITY CERTIFICATION AND ACCREDITATION PROCESS

The following sections describe some of the key activities in an information security program. These activities, including security certification and accreditation, are typically conducted within the system development life cycle. The activities do not necessarily need to be conducted in a sequential manner. In fact, activities can be conducted multiple times or there may be an iterative cycle among selected activities during various phases of the system development life cycle.

Security Categorization

Security categorization standards establish three potential levels of risk (low, moderate, and high) for each of the stated security objectives (confidentiality, integrity, and availability) relevant to securing federal information and information systems. The levels of risk consider both impact and threat, but are more heavily weighted toward impact. The impact is based on the potential magnitude of harm that the loss of confidentiality, integrity, or availability would have on agency operations (including mission, functions, image or reputation), agency assets, or individuals (including privacy). The standards provide federal agencies with a means of determining baseline security controls for their information and information systems. Agencies should consult FIPS Publication 199, *Standards for Security Categorization for Federal Information and Information Systems* (Initial public draft), May 2003, for guidance on categorizing information systems (i.e., selecting appropriate risk levels for those systems).

Risk Assessment

The periodic assessment of risk to agency operations or assets resulting from the operation of an information system is an important activity required by FISMA. The risk assessment brings together important information for agency officials with regard to the protection of the information system and generates essential information required for the security plan. The risk assessment includes: (i) the identification of threats to and vulnerabilities in the information system; (ii) the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability would have on agency operations (including mission, functions, image, or reputation) or agency assets should there be a threat exploitation of identified vulnerabilities; and (iii) the identification and analysis of security controls for the information system. Agencies should consult NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, or other similar publications for guidance on conducting risk assessments.

Security Planning

In accordance with the provisions of FISMA, information security programs are required to have plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate. The preparation of a security plan for an information system ensures that agreed upon security controls planned or in place are fully documented. The security plan also provides a complete characterization or description of the information system as well as attachments or references to key documents supporting the agency's information security program (e.g., configuration management plan, contingency plan, incident response plan, security awareness and training plan, rules of behavior, risk assessment, security test and evaluation results, system interconnection agreements, security authorizations/accreditations, and plan

of action and milestones[21]). Agencies should consult NIST Special Publication 800-18, *Guide for Developing Security Plans Information Technology Systems*, or other similar publications for guidance on creating security plans. Agencies should also consult NIST Special Publication 800-53, *Security Controls for Federal Information Systems*, (Initial public draft projected for publication, Summer 2003), or other similar publications for guidance on selecting security controls.

Security Control Development

For new information systems, the security controls described in the respective security plans are designed, developed, and implemented. For information systems currently in operation, the security plans for those systems may call for the development of additional security controls to supplement the controls already in place or the modification of selected controls that are deemed to be less than effective. This activity typically takes place during the acquisition/development phase of the system development life cycle.

Developmental Security Test and Evaluation

The security controls developed for a new information system must be tested and evaluated prior to deployment to ensure that the controls are working properly and are effective. Some types of security controls (primarily those controls of a non-technical nature) cannot be tested and evaluated until the information system is deployed—these controls are typically management and operation level controls. For those security controls that can be assessed prior to deployment, a security test and evaluation plan is developed. This plan guides the developmental security testing and evaluation of the security controls and provides important feedback to information system developers and integrators. This activity typically takes place during the acquisition/development phase of the system development life cycle.

Security Control Integration

The integration of security controls occurs at the operational site where the information system is to be deployed for operation. Integration and acceptance testing occurs after delivery and installation of the information system. Security control settings and switches are enabled in accordance with manufacturer instructions and available security implementation guidance. This activity typically takes place during the implementation phase of the system development life cycle.

Security Certification

In accordance with the provisions of FISMA, periodic testing and evaluation of the security controls in an information system are required to ensure that the controls are effectively implemented. The comprehensive evaluation of security control effectiveness through established verification techniques and procedures (also known as security certification) is a critical activity conducted by the agency or by an independent third party on behalf of the agency to give agency officials confidence that the appropriate safeguards and countermeasures are in place to protect the agency's information system. In addition to security control effectiveness, security certification also uncovers and describes the actual vulnerabilities in the information system. The determination of security control effectiveness and information system vulnerabilities provides essential information to authorizing officials to facilitate credible, risk-based, security accreditation decisions. Agencies should consult NIST Special Publication 800-53A, *Techniques and Procedures*

[21] The results of security testing and evaluation may uncover deficiencies in the security controls employed to protect an information system. A detailed plan of action and milestone schedule are required to document the planned corrective measures needed to increase the effectiveness of the security controls and provide the requisite security for the information system prior to security authorization. The authorizing official normally reviews and must approve the plan of action and milestone prior to authorizing operation of the information system.

for Verifying the Effectiveness of Security Controls in Federal Information Systems, (Initial public draft projected for publication, Winter 2003-04), or other similar publications for guidance on the evaluation of security controls.

Security Accreditation

In accordance with the provisions of OMB Circular A-130, the security authorization of an information system to process, store, or transmit information is required.[22] This authorization (also known as security accreditation), granted by a senior agency official, is based on the verified effectiveness of security controls to some agreed upon level of assurance and an identified residual risk to agency operations (including mission, functions, image, or reputation) or agency assets. The security accreditation decision is a risk-based decision that depends heavily, but not exclusively, on the security testing and evaluation results produced during the security control verification process. An authorizing official relies primarily on: (i) the completed security plan; (ii) the security test and evaluation results; and (iii) the plan of action and milestones for reducing or eliminating information system vulnerabilities, in making the security accreditation decision on whether to authorize operation of the information system and to explicitly accept the residual risk to agency operations or agency assets.

Configuration Management and Control

Information systems will typically be in a constant state of migration with upgrades to hardware, software, or firmware and possible modifications to the surrounding environment where the system resides. Changes to an information system can have a significant impact on the security of the system. Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation. Ensuring adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment requires an effective agency configuration management and control policy and associated procedures. Configuration management and configuration control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system and subsequently controlling and maintaining an accurate inventory of any changes to the system.

Ongoing Monitoring

In accordance with the provisions of FISMA, periodic testing and evaluation of the security controls in an information system are required on an ongoing basis to ensure that the controls continue to be effective in their application. Security control monitoring (i.e., verifying the continued effectiveness of those controls over time) and reporting the security status of the information system to appropriate agency officials is an essential activity of a comprehensive information security program. The ongoing monitoring of security control effectiveness can be accomplished in a variety of ways including security reviews, self-assessments, security testing and evaluation, or audits. Agencies should consult NIST Special Publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems*, (Initial public draft projected for publication, Winter 2003-04) or other similar publications for guidance on the ongoing monitoring of security controls.

[22] Security authorization is typically only one factor that ultimately goes into the agency decision to place the information system into operation. All functionality within the information system (both security related and non-security related) must be working properly before the final approval to operate is given by the agency's authorizing official.

Figure F.1 illustrates key information security program activities (including security certification and accreditation) and the impact of those activities on the information system.

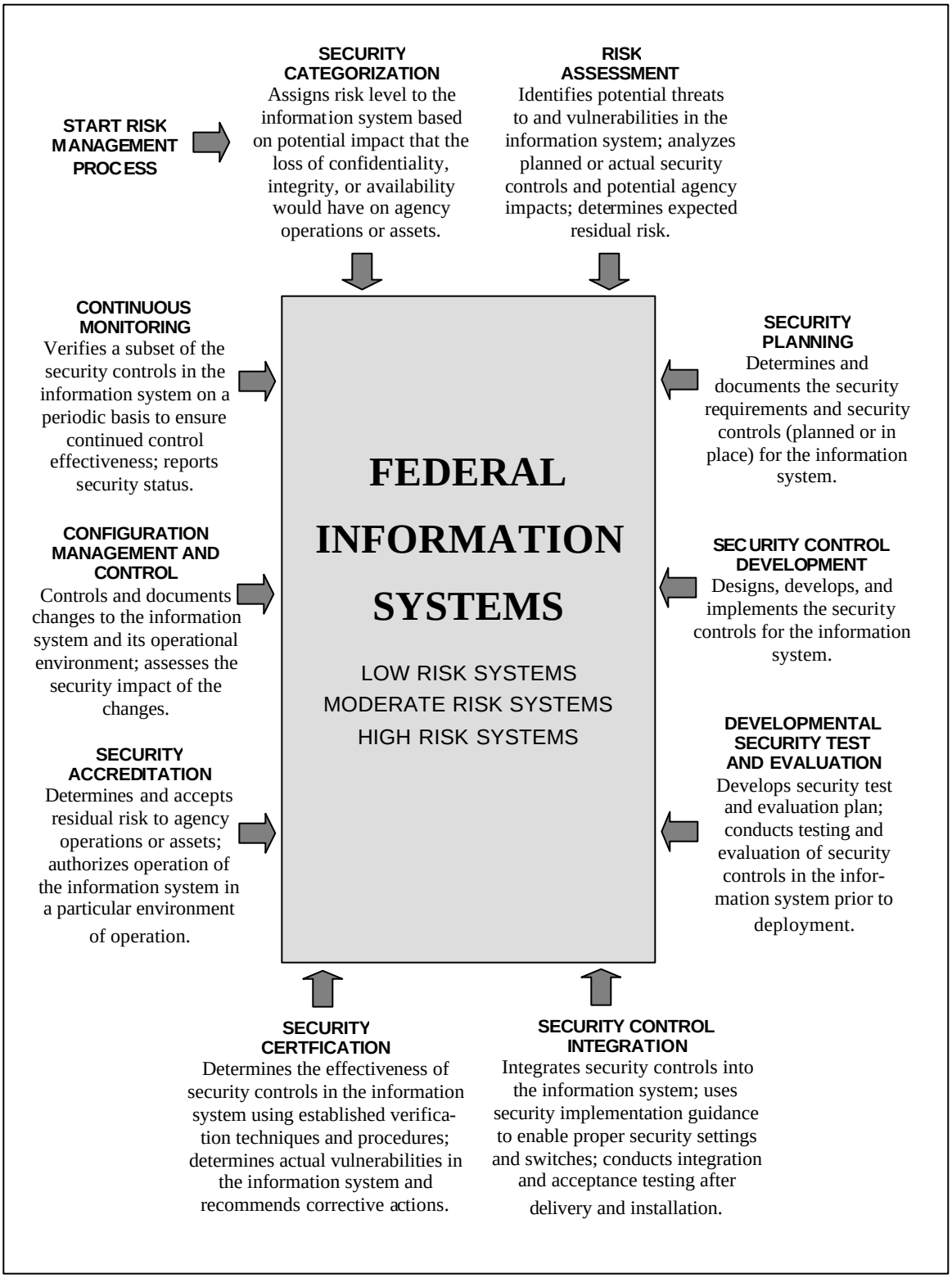

FIGURE F.1 INFORMATION SECURITY PROGRAM ACTIVITIES