FIPS PUB 102

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

1983 SEPTEMBER 27

U.S. DEPARTMENT OF COMMERCE/National Bureau of Standards

GUIDELINE FOR COMPUTER SECURITY CERTIFICATION AND ACCREDITATION

CATEGORY: ADP OPERATIONS
SUBCATEGORY: COMPUTER SECURITY

FIPS PUB 102

U.S. DEPARTMENT OF COMMERCE, Malcolm Baldrige, *Secretary*
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Director*

Foreword

The Federal Information Processing Standards Publication Series of the National Bureau of Standards is the official medium for promulgating standards under the provisions of Public Law 89-306 (Brooks Act) and under Part 6 of Title 15, Code of Federal Regulations. These legislative and executive mandates have given the Secretary of Commerce important responsibilities for improving the utilization and management of computers and automated data processing (ADP) systems in the Federal Government. To carry out the Secretary's responsibilities, the NBS, through its Institute for Computer Sciences and Technology, provides leadership, technical guidance and coordination of Government efforts in the development of guidelines and standards in these areas.

James H. Burrows, *Director*
Institute for Computer Sciences and Technology

Abstract

This Guideline is intended for use by ADP managers and technical staff in establishing and carrying out a program and a technical process for computer security certification and accreditation of sensitive computer applications. It identifies and describes the steps involved in performing computer security certification and accreditation; it identifies and discusses important issues in managing a computer security certification and accreditation program; it identifies and describes the principal functional roles needed within an organization to carry out such a program; and it contains sample outlines of an Application Certification Plan and a Security Evaluation Report as well as a sample Accreditation Statement and sensitivity classification scheme. A discussion of recertification and reaccreditation and its relation to change control is also included. The Guideline also relates certification and accreditation to risk analysis, EDP audit, validation, verification and testing (VV&T), and the system life cycle. A comprehensive list of references is included.

Key words: accreditation; certification; certification/accreditation management; certification/accreditation process; certification/accreditation program; computer security evaluation; EDP audit; Federal Information Processing Standards Publication; recertification/reaccreditation; risk analysis; sensitive computer application; sensitivity classification; validation, verification and testing (VV&T)

Natl. Bur. Stand. (U.S.), Fed. Info. Process. Stand. Publ. (FIPS PUB) 102, 89 pages.
(1984)
CODEN:FIPPAT

For sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161.

Federal Information Processing Standards Publication 102

1983 September 27

ANNOUNCING THE

GUIDELINE FOR COMPUTER SECURITY CERTIFICATION AND ACCREDITATION

Federal Information Processing Standards Publications are issued by the National Bureau of Standards pursuant to the Federal Property and Administrative Services Act of 1949, as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973), and Part 6 of Title 15 Code of Federal Regulations (CFR).

Name of Guideline: Guideline for Computer Security Certification and Accreditation (FIPS PUB 102).

Category of Guideline: ADP Operations, Computer Security.

Explanation: This Guideline describes how to establish and how to carry out a certification and accreditation program for computer security. Certification consists of a technical evaluation of a sensitive application to see how well it meets security requirements. Accreditation is the official management authorization for the operation of the application and is based on the certification process as well as other management considerations. A certification and accreditation program benefits an organization by improving management control over computer security and increasing awareness of computer security throughout the organization.

Approving Authority: U.S. Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

Maintenance Agency: U.S. Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

Cross Index:

a. Federal Information Processing Standards Publication (FIPS PUB) 31, Guidelines for Automatic Data Processing Physical Security and Risk Management.

b. Federal Information Processing Standards Publication (FIPS PUB) 38, Guidelines for Documentation of Computer Programs and Automated Data Systems.

c. Federal Information Processing Standards Publication (FIPS PUB) 39, Glossary for Computer Systems Security.

d. Federal Information Processing Standards Publication (FIPS PUB) 41, Computer Security Guidelines for Implementing the Privacy Act of 1974.

e. Federal Information Processing Standards Publication (FIPS PUB) 46, Data Encryption Standard.

f. Federal Information Processing Standards Publication (FIPS PUB) 48, Guidelines on Evaluation of Techniques for Automated Personal Identification.

g. Federal Information Processing Standards Publication (FIPS PUB) 64, Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase.

h. Federal Information Processing Standards Publication (FIPS PUB) 65, Guideline for Automatic Data Processing Risk Analysis.

i. Federal Information Processing Standards Publication (FIPS PUB) 73, Guidelines for Security of Computer Applications.

j. Federal Information Processing Standards Publication (FIPS PUB) 74, Guidelines for Implementing and Using the NBS Data Encryption Standard.

k. Federal Information Processing Standards Publication (FIPS PUB) 83, Guideline on User Authentication Techniques for Computer Network Access Control.

l. Federal Information Processing Standards Publication (FIPS PUB) 87, Guidelines for ADP Contingency Planning.

m. Federal Information Processing Standards Publication (FIPS PUB) 88, Guideline on Integrity Assurance and Control in Database Administration.

Applicability: This Guideline is a basic reference document for general use by Federal departments and agencies in establishing and carrying out a certification and accreditation program for computer security. Certification and accreditation should be performed for applications that process sensitive data or that could cause loss or harm from improper operation or deliberate manipulation of the application.

Implementation: Certification and accreditation can be performed on computer applications that are operational or under development. Since applications under development can be changed more easily than operational applications, it is more cost effective to start the certification and accreditation process in the development phase of the life cycle; however, the process should be integrated into all phases of the life cycle. In general, the more sensitive the application, the higher the priority for carrying out the certification and accreditation process.

Specifications: Federal Information Processing Standards Publication (FIPS PUB) 102, Guideline for Computer Security Certification and Accreditation (affixed).

Qualifications: This Guideline can help in certifying the sufficiency of security specifications for acquired services, but is not sufficient for such certification. Further regulations and concerns must be considered for such services. The General Services Administration is responsible for providing guidance on procurement activities and can provide further information in this area.

Where to Obtain Copies of this Guideline: Copies of this publication are for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 102 (FIPSPUB102) and title. When microfiche is desired, this should be specified. Payment may be made by check, money order, or deposit account.

Federal Information Processing Standards Publication 102

1983 September 27

Specifications for

GUIDELINE FOR COMPUTER SECURITY CERTIFICATION AND ACCREDITATION

CONTENTS

CONTENTS

CONTENTS

FIGURES

TABLE

SUMMARY GUIDANCE

The best way to view computer security certification and accreditation (sec. 1.2.3,4) is as a form of quality control for the computer security of sensitive applications (i.e., applications with a significant potential for loss). The critical decisions regarding the adequacy of security safeguards in sensitive applications must be made by authorized managers and must be based on reliable technical information. As defined in this document, security certification is a technical evaluation for the purpose of accreditation, and uses security requirements as the criteria for that evaluation; security accreditation is management's approval for operation, and is based on that technical evaluation and other management considerations. It should be noted that computer security certification and accreditation are one aspect of a general certification and accreditation activity that should be performed to assure that a computer application satisfies *all* its requirements. This Guideline tells: A. how to establish a program for computer security certification and accreditation, and B. how to perform such certifications and accreditations. The following summarizes this Guideline. Each section number in parentheses refers to the adjacent topic location in this document.

A. Establishing a Program for Certification and Accreditation

There are six major issues that need to be addressed here. These are briefly described for highly sensitive applications. Less sensitive applications can use less elaborate programs.

1. **Policies and Procedures** (sec. 3.1)

(1) *Program Directive:* should be issued by Senior Executive Officer; should establish official authority for the program; could be part of agency security directive; should contain program summary; should allocate program responsibilities.

(2) *Program Manual:* should be issued by the Certification Program Manager; should define the processes involved; should reflect Certification Program Manager responsibilities; could use this Guideline structure as a basis for the Manual.

2. **Roles and Responsibilities** (sec. 1.3)

The roles enumerated are functional. Particular agencies may have different titles for these functions.

(1) *Senior Executive Officer:* issues the Program Directive; allocates responsibilities.

(2) *Certification Program Manager:* initiates application certification and assigns Application Certification Manager; approves Application Certification Plan; develops and issues the Program Manual; keeps Manual up to date; provides support to Senior Executive Officer and Accrediting Official(s), as needed; reviews and approves Manuals of subsidiary agency components (where they exist); monitors recertification and reaccreditation activities; maintains records on agency certifications and accreditations.

(3) *Application Certification Manager:* develops Application Certification Plan for a certification; manages the security evaluation; produces the security evaluation report; periodically reports to management on certification status.

(4) *Security Evaluator:* performs the technical security evaluation necessary for the certification; is located in the appropriate agency office (e.g., standards and quality control office, security office, Inspector General office).

3. **Entities Requiring Certification/Accreditation** (sec. 1.2.7, app. C)

The determination of which applications require certification and accreditation is based on application sensitivity. Sensitivity is measured by the potential loss or harm caused by a security failure. It is desirable to have a prioritized listing, based on mission needs, of those applications that require certification and accreditation.

4. **Organization Structure Concerns** (sec. 3.2)

Each organization must develop its own structure for successful certifications. Two caveats are:

(1) The more sensitive the application, the higher the management level of the Accrediting Official(s).

(2) Security evaluators must be as independent of the sensitive application as possible.

5. **Scheduling** (sec. 1.4)

Ideally, the certification and accreditation process should be integrated into the stages of the system life cycle (i.e., requirements definition, development, operation, and maintenance). The most cost effective use of this process occurs in the requirements definition and development stages.

6. **Staffing, Training, and Support** (sec. 3.3)

Adequate staffing, training, and support for the process is necessary for achieving effective computer security of sensitive applications. This implies the need for career paths for security staff, proper training of security personnel, and suitable funding for security activities.

B. Performing a Certification and Accreditation

1. Certification

Certification consists of a technical evaluation of a sensitive application to see how well it meets its security requirements. The process can be described with five steps:

(1) *Planning* (sec. 2.1): This involves performing a quick and high-level review of the entire system to understand the issues; placing boundaries on the effort; partitioning the work within those boundaries; identifying areas of emphasis; and drawing up the Certification Plan.

(2) *Data Collection* (sec. 2.2): Critical information that needs to be collected includes: system security requirements; risk analysis data showing threats and assets; system flow diagrams showing inputs, processing steps, and outputs plus transaction flows for important transaction types; and a listing of application system controls. If this information is not available in documents, it should be obtained from application personnel by use of tutorial briefings and interviews.

(3) *Basic Evaluation* (sec. 2.3): A basic evaluation is always performed in a certification. Its four tasks are:

a. Security Requirements Evaluation—Are these documented and acceptable? If not, they must be formulated from requirements implied in the application, and compared with Federal, state, organizational and user requirements.

b. Security Function Evaluation—Do security functions (e.g., authentication, authorization) satisfy security requirements? This review should be performed down through the functional specification level.

c. Control Implementation Determination—Check that security functions have been implemented. Physical and administrative controls require visual inspection; controls internal to the computer require testing.

d. Methodology Review—Review the acceptability of the implementation method (e.g., documentation, project controls, development tools used, skills of personnel).

(4) *Detailed Evaluation* (sec. 2.4): In application areas where a basic evaluation does not provide enough evidence for a certification, one analyzes the quality of the security safeguards using one or more of three points of view:

a. Functional Operation—Do controls function properly (e.g., parameter checking, error monitoring)?

b. Performance—Do controls satisfy performance criteria (e.g., availability, survivability, accuracy)?

c. Penetration Resistance—Can controls be easily broken or circumvented? (Establishes confidence in safeguards.)

In conjunction with or in addition to the above, one can gain valuable insight and develop useful examples by focusing on analysis of security relevant components (e.g., assets, exposures), or on situational analysis (e.g., attack scenarios or transaction flows).

(5) *Report of Findings* (sec. 2.5): This is the primary product of a certification. It contains both technical and management security recommendations. It should summarize applied security standards or policies, implemented controls, major vulnerabilities, corrective actions, operational restrictions, the certification process used, and should include a proposed accreditation statement.

2. **Accreditation** (sec. 2.6)

Accreditors use the certification report to help evaluate certification evidence. They then decide on the acceptability of application security safeguards, approve corrective actions, insure that corrective actions are implemented, and issue the accreditation statement. While most flaws will not be severe enough to remove an operational system from service, they may require restrictions on operation (e.g., procedural security controls).

3. **Recertification and Reaccreditation** (sec. 2.7)

As security features of a system or its environment change, recertification and reaccreditation are needed. The more extensive these changes are, the more extensive the recertification and reaccreditation activity should be (i.e., more complete reevaluation, use of higher level Accrediting Official(s)). The change control (configuration management) function is a suitable area in which to place the monitoring activity for these changes.

4. Evaluation Techniques for Security Certification (sec. 1.5)

There are four groups of techniques currently used for security evaluation that can be used for certification.

(1) *Risk Analysis:* This is used to understand the security problem by identifying security risks, determining their magnitude, and identifying areas needing safeguards. When performed at the beginning of the system life cycle, it can provide the basis for security requirements. When performed later in the life cycle, it can be used as an evaluation for security certification.

(2) *Validation, Verification, and Testing:* Validation determines the correctness of a system with respect to its requirements; verification checks for internal consistency during implementation; and testing uses data to examine system behavior. VV&T applied to security requirements becomes an evaluation technique for security certification.

(3) *Security Safeguard Evaluation:* These methods assess the security solution using aids such as checklists, control matrices, and weighted ratings for levels of security produced by different combinations of controls. A security officer may head such an evaluation. It can be the major contributor to evaluation for a security certification when security requirements are the criteria used.

(4) *EDP Audit:* These methods assess whether controls satisfy management's control objectives (a form of requirements) and use the same aids as in security safeguard evaluation. In addition to security controls, however, EDP audit may address cost and efficiency in meeting mission objectives. When the controls that are reviewed are supposed to satisfy management's control objectives for security, an EDP audit becomes a form of evaluation for a security certification.

1. INTRODUCTION

Some computer security risks threaten the very existence of an organization. Critical decisions regardng the adequacy of security safeguards in sensitive applications must be made by authorized managers and must be based on reliable technical information. Computer security certification gives managers this technical information and computer security accreditation gives them the structure needed to make such critical decisions. Together they provide management with a quality control technique for computer security. A second major advantage of such a certification and accreditation program is the increased security awareness that is simultaneously dispersed throughout the organization.

The management control and security awareness provided by a computer security certification and accreditation program can yield major benefits. These processes can help protect against fraud, illegal practices, mission failures, embarrassing "leaks," and legal action. They can help keep managers from being "surprised" by problems within their sensitive computer applications. Computer security certification and accreditation are only one aspect of a general certification and accreditation activity that should be performed to assure that a computer application satisfies its defined functional, performance, security, quality, and reliability requirements. While the guidance here focuses on those aspects of this general process relevant to the computer security of an ADP application, it should be realized that computer security certification and accreditation activities are best accomplished as part of an overall certification and accreditation effort that addresses all the types of requirements and that often uses the same techniques for performing technical evaluations. Discussion of this general certification and accreditation process is beyond the scope of this Guideline, however.

The need for computer security certification has been widely publicized. The need for computer security accreditation is implied by the [FIPS39] definition for certification. The guidance in this document can be used in accomplishing these certifications, accreditations, recertifications, and reaccreditations. This Guideline can also help in certifying the sufficiency of security specifications for consultant services. Further regulations and concerns must be considered, however, for such services. The General Services Administration is responsible for providing guidance on procurement activity and can provide further information in this area.

1.1 Purpose and Audience

The primary purpose of this document is to provide a guideline for establishing both a program and a technical process for certifying and accrediting sensitive computer applications. Subsidiary objectives of this Guideline are:

1. Provide the information and insight to permit readers to adapt or formulate a program and/or process suited to their specific needs.

2. Catalyze increased security awareness and help ensure more appropriate assignment and assumption of security responsibility.

3. Create an awareness of the need for defining security requirements and evaluating compliance with them.

4. Help ensure that computing resources and sensitive information are appropriately protected.

5. Help reduce computer fraud and related crimes.

This Guideline is directed primarily towards those responsible for performing computer security certification and accreditation and those responsible for establishing certification and accreditation programs, i.e.,

1. Senior Executive Officers (e.g., Department Secretary).
2. Accrediting Officials (e.g., senior managers).
3. Computer Security Staff (e.g., managers, system/ADP security officers, internal control specialists).
4. Application Sponsors (e.g., users, resource managers).
5. Independent Reviewers (e.g., financial and EDP auditors, computer quality assurance personnel, test and evaluation personnel).
6. Suppliers of ADP Services (e.g., ADP installation managers, data base administrators, communications officers).
7. Development Staff (e.g., programmers, designers).

1.2 Primary Definitions

Seven definitions are presented and discussed in this section: computer security, computer security requirement, computer security certification, computer security accreditation, computer system, computer application, and sensitive computer application. Definitions of other relevant terms are included in Appendix A. Those definitions without references were formulated in the preparation of this Guideline. Others, as noted, were adapted from existing definitions.

1.2.1 Computer Security[1]

> The quality exhibited by a computer system that embodies its protection against internal failures, human errors, attacks, and natural catastrophes that might cause improper disclosure, modification, destruction, or denial of service.

Three points are key. First, the computer security of a system or application is a relative quality, not an absolute state to be achieved. Second, computer security is concerned with four equally important exposure categories: disclosure, modification, destruction, and denial of service. Third, these exposures are not restricted to data. For example, they can also apply to hardware.

1.2.2 Security Requirement

> An identified computer security need.

These needs derive from governmental policy, agency mission needs, and specific user needs. Governmental policy relating to computer security is expressed in laws and regulations; agency security needs are found in the agency's standards and policy; and user security needs originate in the application characteristics (and might be found in the Project Request Document). Security requirements are expressed in increasing detail as one progresses from high-level general descriptions of the system through lower levels of detailed specification. Evaluation for security certification focuses on the determination of compliance with security requirements. Security requirements need frequent review to insure their accuracy.

[1] This Guideline uses the terms 'computer security' and 'security' synonymously.

1.2.3 **Certification**[2] [FIPS 39]

> The technical evaluation, made as part of and in support of the accreditation process, that establishes the extent to which a particular computer system or network design and implementation meet a prespecified set of security requirements.

Two points are important. First, certification is a technical process that produces a judgment, a statement of opinion. It is not a guarantee. Second, certification complements the accreditation process, defined in the next section.

1.2.4 **Accreditation**[3] [FIPS 39]

> The authorization and approval, granted to an ADP system or network to process sensitive data in an operational environment, and made on the basis of a certification by designated technical personnel of the extent to which design and implementation of the system meet prespecified technical requirements for achieving adequate data security.

Accreditation is thus official management authorization for operation. Although the definition refers to ''data security'' and the processing of ''sensitive data,'' this Guideline assumes that the definition also applies more broadly to computer security in general and to sensitive computer applications that might not contain sensitive data. Such applications might be sensitive due to loss or harm that could result from operational failure (denial of service), rather than from unauthorized disclosure or manipulation of data.

1.2.5 **Computer System**

> An assembly of elements including at least computer hardware and usually also computer software, data, procedures, and people, so related as to behave as an interacting or interdependent unity. [Adapted from FIPS11, NBS80, SIP72, and WEB76]

It is important that the notion of computer system include all aspects that affect security. For this reason, the definition includes not only hardware, software, and data, but also procedures and people.

1.2.6 **Computer Application**

> The use(s) for which a computer system is (are) intentionally employed. [Adapted from SIP72]

The term ''certification'' has been applied to software programs, hardware components, applications, systems, terminals, networks, installations, and other entities. The nature of the entity being certified, however, has minimal effect on the general certification and accreditation processes as described herein, although it has substantial effect on the details of particular certifications. The term ''application'' is broadly defined to represent a variety of certification entities corresponding to a variety of computer systems. For example, an application might encompass one or several computers or sites, although typically there are several applications using a single computer. Application boundaries are determined uniquely for each situation, and are discussed in Section 2.1.2.3.

[2] This Guideline uses the terms 'security certification' and 'certification' synonymously.

[3] This Guideline uses the terms 'security accreditation' and 'accreditation' synonymously.

1.2.7 **Sensitive Computer Application** [OMB78]

> A computer application which requires a degree of protection because it processes sensitive data or because of the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation of the application.

All computerized applications have some degree of sensitivity. The important issue here is that there be agreement within the agency on which applications require certification and accreditation. A prioritized listing of these is desirable.

The appropriate measure of sensitivity is expected loss or harm in light of perceived threats. It is often derived from a risk analysis. Application sensitivity is influenced by many factors, several of which are not self evident. The more obvious factors include such things as mission importance, asset value, and anticipated threats. Less evident factors are the number of users, the range in sensitivity of user positions, and the extent of users' functional capabilities, with the spectrum extending from the limited ability to use only function keys to the other extreme of full user programming. [FIPS73] gives examples of sensitive applications.

Sample categorization schemes for application sensitivity are shown in Appendix C. Such a scheme influences certification and accreditation in several ways. It influences the organizational level of the Accrediting Official(s), with higher sensitivity typically warranting a more senior individual(s); and it influences the level of detail, frequency, and nature of the certification process. For example, highly sensitive applications are reviewed more thoroughly and more often, and require more definitive evidence than applications with low sensitivity.

1.3 Roles and Responsibilities

Within an agency, the Senior Executive Officer (e.g., Department Secretary) has ultimate responsibility for ensuring that agency data and resources are appropriately protected. This responsibility carries with it the responsibilities for establishing agency security policy, enforcing compliance with policy, and ensuring the quality of the agency security program. A certification and accreditation program is an important part of an agency security program. The emphasis that the Senior Executive Officer places on fulfilling these responsibilities has a strong influence on the success of the certification and accreditation program. (See Section 3 for details on establishing the program.)

Four key responsibilities are necessary in carrying out a certification and accreditation program. These responsibilities are: (1) to accredit specific applications, (2) to manage the overall agency program, (3) to manage individual certification efforts, and (4) to perform technical security evaluation. This Guideline defines four roles corresponding to these responsibilities: (1) Accrediting Official, (2) Certification Program Manager, (3) Application Certification Manager, and (4) Security Evaluator. It is not necessary for an agency to adopt these roles by name. They are used here to simplify discussion. It is necessary, however, that the responsibilities be assigned. This section describes the four responsibilities (in terms of the roles) and presents criteria for selecting the people assigned to fulfill them. Appendix G presents an example that shows a sample organizational structure for these roles.

1.3.1 **Accrediting Official**

The Accrediting Officials are the agency officials who have authority to accept an application's security safeguards and issue an accreditation statement that records the decision. The Accrediting Officials must also possess authority to allocate resources to achieve acceptable security and to remedy security deficiencies. Without this authority, such individuals cannot realistically take responsibility for the accreditation decision. In general, this requires the Accreditors to include a senior official and perhaps the line manager for the application in question. For some very sensitive applications the Senior Executive Officer is appropriate as an Accrediting Official. In general the more sensitive the application, the higher the Accrediting Officials are in the organization.