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.

An Accrediting Official or group of Officials might be responsible for several applications, but for each application, there is typically only one Accrediting Official or group of Officials assigned. For example, some Department of Defense (DoD) applications require more than one Accrediting Official. This occurs because several DoD agencies serve as custodians for particular types of information and each must approve the security safeguards of applications that process this information.

Where privacy is a concern, Federal managers can be held personally liable for security inadequacies. The issuing of the accreditation statement fixes security responsibility, thus making explicit a responsibility that might otherwise be implicit. It also shows that due care has been taken for security. Accreditors should consult the agency general counsel to determine their personal security liabilities.

1.3.2 Certification Program Manager

The Certification Program Manager is responsible for defining and managing the security certification program within an agency. While the details of this role might vary widely, at a minimum it involves producing agency specific certification guidance and periodically reporting to management on program status. It might also involve active oversight of certifications. (See Appendix G for an example that enumerates a possible set of responsibilities.)

There is typically one Certification Program Manager designated within an agency. If the agency includes somewhat autonomous subsidiary components, such as the Public Health Service or the Social Security Administration within the Department of Health and Human Services, these components might also have individuals designated to manage the component certification programs. The role of Certification Program Manager can be assigned to the Agency ADP Security Officer. It might also, along with the security officer role, be assigned to the Information Resources Management office.

The individual selected to fill this role should possess substantial knowledge of agency structure, politics, agency program, mission objectives, and capabilities as well as general knowledge of ADP and security. The role is that of a management professional rather than a technical analyst.

1.3.3 Application Certification Manager

The Application Certification Manager is responsible for managing a specific certification effort. This individual plans the effort, procures evaluation resources, and oversees production of the security evaluation report. The person selected as Application Certification Manager is as independent as possible from the application being certified, to help ensure an objective evaluation. Ideally this person is familiar with the application requirements and technology, as well as generally-accepted computer security safeguards. (See Appendix G for an example that enumerates a possible set of responsibilities.)

In some cases, several certification efforts are performed in support of one accreditation decision. This can arise due to the partitioning of organizational responsibilities into several technical security areas. In such cases, it is preferable to integrate the technical certification findings into one final report, since the safeguards in each area can have complex interrelationships that require a technical interpretation.

1.3.4 Security Evaluator

Security Evaluators perform the technical security evaluation tasks. Their responsibility is to provide expert technical judgments in their areas of specialization. Required Security Evaluator specializations vary with each application. For basic (high-level) evaluations, computer security generalists with some application-specific training are sufficient. For detailed evaluations, greater specialization is required. Useful specialties include: application analysts, systems analysts, engineers, designers, application programmers, systems programmers, testers, contract specialists, and lawyers. For detailed developmental certifications, Security Evaluator skill requirements vary with the developmental phases, as shown in Appendix F. Security evaluation is typically best performed by a team, since this provides the advantage of combined skills and viewpoints.

As implied above, Security Evaluators are as independent as possible from the application. Nevertheless, while security evaluation requires a degree of independence to help ensure objectivity, a fully independent evaluation is not feasible in many cases. In some areas it is necessary and reasonable to accept the technical judgments of application developers and users. Furthermore, every application has people associated with it who are already aware of many of its flaws. For example, system programmers are usually aware of operating system shortcomings. While these people might not have the authority or resources to correct deficiencies, their expertise should be sought in identifying the deficiencies. The Application Certification Manager must weigh the benefits of independence against its increased expense, and arrive at an appropriate mix.

1.3.5 **Responsibilities Of Agency Offices**

Many agency offices should support the certification program. It is especially important that offices associated with the application being evaluated cooperate with and support certification efforts. They must provide briefings, interviews, and documentation as requested. They might be required to prepare application flow charts and control listings and to complete questionnaires or checklists. They might also be required to assist in the preparation of security requirements and risk analyses. They should also be responsible for informing appropriate authorities on the initiation of a development effort and on the occurrence of events such as violations or errors in operational applications that might require or affect certification. It is useful to assign an application person as the point-of-contact for the certification team.

Primary support from other offices is through the loan of personnel to provide security evaluation support or, where this is not possible, through the direct performance of evaluation tasks for the certification effort. Agency review offices such as the ADP portion of the Office of the Inspector General (OIG), ADP Security Office, ADP quality assurance and standards, and test and evaluation are key providers of independent technical evaluation support. Some of their own internal work also provides certification evidence. The major example is the evaluation of application compliance with internal security-relevant policies or standards that were formulated by these offices (e.g., audit requirements, developmental standards, measures-of-test-coverage standards). For the most cost effective security evaluation support, quality assurance and VV&T (Validation, Verification, and Testing) should be provided for in the planning phase of an application's development.

It is important to distinguish between the certification and accreditation program and the duties of the OIG. Auditors do not serve as Accrediting Officials, since this would impair the auditors' independence. The auditors' main certification support responsibilities are: (1) to provide technical evaluation, as required, in assessing control adequacy and auditability and (2) to inform appropriate authorities of situations that might require or affect certifications. Auditors often obtain certification relevant findings which should be forwarded to certification program personnel.

1.4 Considerations for Scheduling

Certification and accreditation can be performed on applications that are operational or under development. For several reasons, it is preferable to perform initial certification and accreditation when an application is under development. First, it is easier to change an application under development than one that has been in operation for a period of time. Second, it is easier to prevent a severely flawed application from becoming operational than to remove it from an operational state. A number of factors underlie this.

1. *Resistance to change.* People resist change. This is true of changes to any operational system but can be especially applicable in security relevant cases, since the change might add procedural steps, restrict existing capabilities, restrict flexibility, increase application response time, or remove capabilities previously present. There is resistance to change during development, also, but the amount of resistance is usually less since there is no large entrenched constituency.

2. *Costs.* Financial and technical resources required to make security changes to an operational application are far greater than those required to make similar changes during development. Some estimates place the costs for changes during operation as being at least thirty times higher [GA082-1, p. 29].

3. *Lack of exploitation evidence.* It might be difficult to justify the correction of even a major flaw if an application has been operational for years without evidence of the flaw being exploited. Sometimes the absence of exploitation evidence might indeed be valid ''proof'' that the threat is not sufficient to warrant increased safeguards. The lack of evidence, however, does not ensure that the flaw is not being or will not be exploited. In addition, many computer security flaws are such that even one exploitation could have disastrous effects. This is especially true in the contingency planning area [FIPS87].

Another reason for performing certification and accreditation during development is that it permits the development process itself to be changed. For example, if certification analysis shows development quality to be insufficient, strict programming standards can be adopted. Developers might be requested to provide evidence of security analysis.

It is worth emphasizing that the above arguments can be overridden. The most important criterion in deciding which certifications and accreditations to perform first is application sensitivity (as might be reflected in a prioritized listing of agency applications by sensitivity). If the greatest sensitivity is possessed by an operational application, it should generally be the first to be examined. Even here, however, there are other factors to consider. For example, certification of a low sensitivity application might be scheduled before certification of a high sensitivity one in order to acquire needed training and increase technical proficiency. The point here is that, though situational needs must be considered, it is usually best to initially certify and accredit applications while they are under development. This is in keeping with the principles of life cycle management, and ensures that major certification influence occurs during the ''formative'' period in an application's life. Appendix F shows how certification and accreditation activities are interleaved with application development.

1.5 Evaluation Techniques for Security Certification

Evaluation of computer security is an activity that has slowly been growing in importance and is performed in four communities affected by computer security issues. These communities are the ones that perform: 1) risk analysis, 2) validation, verification, and testing (VV&T), 3) security safeguard evaluation, and 4) EDP audit. Each of these communities has many approaches to evaluation of security and performs these evaluations for different purposes. A security evaluation performed for certification is characterized by using security requirements as criteria or the baseline for evaluation. When any one of the above communities uses security requirements as criteria for evaluation, their evaluation can be used for certification.

Evaluation for certification involves validating security requirements, examining safeguards or controls, and determining whether safeguards satisfy requirements. Primary emphasis is on requirements and safeguards rather than on threats, assets, and expected losses. Methods of evaluation used in each of the four communities cited above can be adapted for use as evaluations for certification. The integration of these adapted methods into the certification process described in this Guideline is a large component of this computer security technique named ''certification and accreditation.''

A certification begins by reviewing the requirements for acceptability. In areas where threats and expected losses are well understood, risk analysis methods can be used. Where threats and expected losses are not well understood, evaluation aids for certification such as security checklists or control reviews can be used. The objectives of this type review are summarized in Section 2.3.1. Security safeguard evaluations and EDP audit methods can be used to select additional security requirements when the evaluation used for certification finds the application lacking in some area.

If no security requirements have been explicitly formulated when certification begins, the certification team must come up with such a formulation in order to perform an evaluation for certification. Risk analysis data can be used for this purpose.

As the application development process unfolds in the application life cycle, the certification process determines whether controls satisfy security requirements, and does this at different levels of specificity. As described in Section 2.3, the minimum level of evaluation for certification is a 'basic evaluation' and includes reviewing the functional specifications against security requirements. For areas of the application that need in-depth security assessment, a 'detailed evaluation' is performed, as described in Section 2.4. As appropriate, the various groups of security evaluation methods are called upon to provide these reviews.

During the operation and maintenance of the application, recertification and reaccreditation will eventually be needed. This means that an evaluation for recertification must occur. Recertification evaluation is similar to a certification evaluation but takes place more selectively since areas of the application that experience no changes need no action. Note that an operational application that has never been certified is a candidate for certification, not recertification.

The following briefly describes and compares the four groups of security evaluation methods that can be used for certification evaluation.

1.5.1 Risk Analysis

1.5.1.1 Its Uses—The primary purpose of risk analysis is to understand the security problem by identifying security risks, determining their magnitude, and identifying areas where safeguards or controls are needed. It can also be used to determine how many resources to budget for security and where to allocate these resources. It is best performed at the beginning of the system life cycle and, with user inputs and policy requirements, can provide the basis for choosing system security requirements (Phase I in fig. 1-1).

Risk analysis can also be useful in validating requirements (Phase IIA in fig. 1-1). If requirements are defined to the functional safeguards level, risk analysis can be used to determine whether the protection embodied in the controls reduces expected loss to an acceptable level at acceptable cost (Phase IIB in fig. 1-1). This is typically done by estimating reduced threat frequencies or damages based on the presumed implementation of the identified safeguards. Risk analysis thus plays a dual role in any certification program because it can be used both to help determine important security requirements (the criteria for the process of certification) and to evaluate the safeguards.

Some further things to note about risk analysis are: (1) risk analysis is a stand-alone process that can be performed independently of a certification; (2) it is usually performed under the direction of people internal to the system in question; and (3) risk analysis becomes an evaluation technique for certification when a particular level of loss becomes an acceptable security requirement of the application. Figure 1-1 shows the relation of certification and risk analysis to the application's life cycle. For examples of risk analysis methods see [FIPS65], [SDC79], [IST79], and [HOF80]. For a discussion of risk analysis methods and brief descriptions of them see [NBS83]. Note that [OMB78] requires risk analysis as well as certification for sensitive applications.

1.5.1.2 Its Limitations—Theoretically, risk analysis can be used to examine the effectiveness of any control by determining its impact on expected loss. This holds true in areas such as environmental security, where reliable data exist on threats such as fires and floods and the losses they might cause. In situations where reliable data do not exist on threat frequencies and expected losses, it is extremely difficult to evaluate safeguards in such terms and so accuracy of the findings diminish. For example, it is difficult to determine whether and to what extent the addition of a software safeguard will reduce the threat from a system penetrator. Similarly, although the addition of authentication safeguards reduces expected losses from unauthorized access, it is difficult to specify the extent of this reduction. This reduced accuracy applies not only to analyzing less understood controls but also to analyzing technically detailed safeguards such as those that are not visible above the level of the application specification.

Life Cycle Phase	*Security Concern*	*Preferred Security Process to be Applied*
I. INITIATION	A. Understand the security problem: identify security risks; determine their magnitude; identify areas where safeguards are needed.	Risk Analysis
	B. Define security requirements.	
II. DEVELOPMENT DEFINITION DESIGN PROGRAMMING TESTING	A. Validate security requirements.	Risk Analysis VV&T
	B. Assess recommended and implemented safeguards; determine whether they satisfy requirements.	Certification
	C. Approve for operation.	Accreditation
III. OPERATION AND MAINTENANCE	A. Reassess security risks.	Risk Analysis Safeguard Eval. EDP Audit
	B. Reassess safeguards.	Recertification*
	C. Approve for continued operation.	Reaccreditation

*If risk analysis, VV&T, certification and accreditation were not performed during development, they might be performed initially during operation. It is far preferable to perform them during development, however.

Figure 1-1. *Life cycle phases and security processes*

The basic problem in using risk analysis to examine controls lies not in risk analysis itself, but in the use of expected loss as an evaluation baseline. As the impact of safeguards on expected losses becomes less clear, expected loss becomes a less meaningful measure of a safeguard's acceptability. What is needed in evaluating controls is a different baseline against which more objective evaluations can be made. The best baseline for this is that provided by the security requirements themselves. That is why a certification evaluation is the technique being recommended.

1.5.2 Validation, Verification, and Testing (VV&T)

VV&T is a process of review, analysis, and testing that should be performed on a system throughout its life cycle but is particularly cost effective when performed during the early life cycle. Validation determines the correctness of the system with respect to its requirements; verification checks the internal consistency and completeness of the system as it evolves and passes through different levels of specification; and testing, either automated or manual, examines system behavior by exercising it on sample data sets. The performance of VV&T provides a powerful quality assurance technique for applications, and when application requirements include security, VV&T becomes an important evaluation technique for security certification. VV&T is usually performed by the people responsible for developing the application; however, for critical applications it may be done by an independent body.

To save on costs, it is important to draw upon evaluation activities in the application life cycle process itself in order not to duplicate such efforts. Applications that are being developed or have been developed with quality assurance in mind will have a VV&T program interleaved in the life cycle process. For example, the validation activity checks the correctness of a system against its security requirements when such requirements are explicitly stated (Phase IIA, fig. 1-1). Evaluation for certification can also draw heavily on other VV&T evidence, when it exists, and thereby reduce evaluation costs considerably (Phase IIB, fig. 1-1). For further information on VV&T see [FIPS101].

1.5.3 Security Safeguard Evaluation

Security safeguard evaluation is an umbrella term being used here for security evaluations performed by people independent of the application in question but internal to the organizational division in which the application resides. A security officer may head such an evaluation. Security evaluations of this type can be the major contributors to evaluation for certification, particularly since it is recommended that the Accreditor or one of the Accreditors (if there is a group performing this function) be a manager responsible for the application. The organizational proximity of the security evaluators and the Accreditor suggested here makes this type evaluation an internal approach to managing the application and may be the most effective arrangement possible.

These evaluation methods usually partition the problem into manageable pieces that correlate with the different skill areas or organizational entities involved in the application. For example, the security checklist used by the Department of Defense [DoD79] partitions the problem into: security management, physical facilities, personnel, hardware, software security, service personnel, files, internal audit controls, time-resource sharing, contingency plan, and use of service bureaus. Within each area, controls are examined and assessed so that an overall picture of the security posture emerges. Examples of different approaches are checklists [AFI79] [DoD79], control matrices [FIT78], and partially quantitative evaluations that assign weights and ratings to the levels of security achieved by the various controls [PMM80]. There are numerous such methods in use but there is no one method suitable for all applications. For further examples and an in-depth discussion of these methods see [NBS83]. Since this group of evaluation methods has comprehensive lists of controls to look for in evaluating the security posture of an application, it can also be used for determining additional security requirements as well (Phase IIIA, fig. 1-1). Just as with risk analysis, these methods can serve the dual purposes of 1) helping determine security requirements and 2) evaluating safeguards.

1.5.4 EDP Audit

EDP audit, a subdiscipline within internal audit, assesses the controls in an organization's system that rely on computers. It determines how well these systems are complying with management's control objectives for these systems and reports its findings to upper management. When control objectives for security (a high-level form of security requirement) are considered, EDP audit becomes a form of security evaluation usable for certification. However, since EDP audit is usually located outside the organizational unit responsible for the application in question, and, since it usually has a broader scope than security, EDP audit would usually be a secondary contributor to a certification evaluation. Since EDP audit methods typically identify a comprehensive set of controls, they can be used for helping determine security requirements as well (Phase IIIA, fig. 1-1). There are numerous EDP audit methods that have been developed by auditing firms and the U.S. General Accounting Office. Some examples are [AAC78], [MAI76], [PMM80], [CIC75], and [GAO81-2,3]. For further discussion of these methods see [NBS83].

1.5.5 Comparison Of Security Safeguard Evaluation And EDP Audit

With respect to the technical processes themselves, security safeguard evaluation and EDP audit have many similarities. For example, both assess compliance with policies; both assess the adequacy of safeguards; both include tests to verify the presence of controls. However, since EDP audits are generally broader in scope (e.g., part of a general internal review), EDP audits often address issues, such as cost and efficiency in achieving mission objectives, that are outside the purview of evaluations for certifications.

The primary difference between security safeguard evaluation and EDP audit is that safeguard evaluation takes place within the bounds of application responsibility, whereas EDP audit usually takes place outside these bounds. EDP audit is usually not performed under the oversight of an application manager. Furthermore, EDP audit findings for an application are typically reported at a higher level than the person directly responsible for the application. It is an external evaluation procedure used by higher-level managers in managing the agency.

Beyond these differences, there are others of a more subtle nature. For example, EDP audits in general place more emphasis on data reliability [GAO81-3] and validate the data processed by the application (i.e., "substantive" testing). In a security safeguard evaluation, file inconsistencies are of interest mainly to the extent that they reveal inadequacies in the safeguards. As another example, EDP audits tend to be concerned with threats anticipated by application developers and thus tested for in the application and in audit journals. Security safeguard evaluations, while also concerned with anticipated threats, are often additionally concerned that safeguards counter threats in which the application is used in ways not anticipated or intended by its developers. Penetration of an application through a design flaw is an example of an unanticipated threat. Analyses of these two forms of threats require different skills.

As both EDP audit for security and security safeguard evaluation evolve, some differences are lessening and more overlap of concerns is occurring. For example, the historical limitation of EDP audits to financial concerns is diminishing, as is the historical limitation of security safeguard evaluation to violations associated with unauthorized disclosure. EDP audits are being broadened to consider the entire spectrum of computer applications that are being used to manage agency information resources; and security safeguard evaluations increasingly consider exposures such as agency embarrassment or competitive disadvantage that were formerly primarily of concern to auditors. Differences expected to remain, however, are that EDP audit will continue to be broader in scope and will remain a review external to the application whereas security safeguard evaluation will remain a review internal to the application location in the organization.

2. PERFORMING CERTIFICATION AND ACCREDITATION

This section presents guidance on performing certification and accreditation. It applies to certifications performed during either development or operation. Recertification and reaccreditation are also discussed. The section is organized as follows:

2.1 Planning. What preliminary steps are needed before the central part of the evaluation activity can begin? How much evaluation depth is needed?

2.2 Data Collection. How is information gathered for evaluations?

2.3 Basic Evaluation. What is involved in performing a basic security evaluation for certification? What evaluation methods are applicable?

2.4 Detailed Evaluation. What is involved in a detailed evaluation? What methods are applicable to detailed evaluation? How can evaluation analysis be focused?

2.5 Report of Findings. What does the security evaluation report contain?

2.6 Accreditation. What issues are considered in making the accreditation decision? What does the accreditation statement contain?

2.7 Recertification and Reaccreditation. When are recertification and reaccreditation needed? What activities are involved? How are changes controlled?

Figure 2-1 summarizes the certification process. It is an iterative process. That is, based on findings from each stage, previous stages might have to be reentered and work performed over. For example, basic evaluation might identify a function that is not included within evaluation boundaries but that is important for security. This can require revision of the boundaries defined during planning, along with additional data collection.

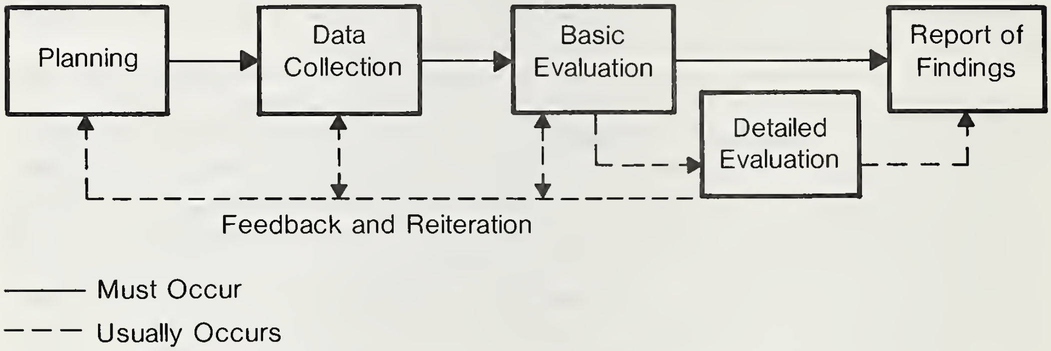


Figure 2-1. *The certification process*

The work is not as sequential as the figure suggests. Typically most or all of the stages are ongoing at the same time. The intent of the figure is to show the shift in emphasis as work progresses.

''Basic'' evaluation means ''high-level'' or ''general'' evaluation and is the minimum necessary for a certification to take place. In general, basic evaluation suffices for most aspects of an application under review. However, most certifications also require detailed work in problem areas, and therefore require detailed evaluation as well.

Time and resources required to perform a certification vary widely from case to case. In all cases, however, a balance must be kept between potential security risks and certification costs. If possible loss or harm is low, certification costs must also be kept low. Risk analysis can help in deciding how much certification review an application can afford. Typical resources for certification can vary from several person-days to many person-months. Minimum products required from certification and accreditation are a security evaluation report and an accreditation statement.

The certification process described here takes the form of a functional description. It tells what must be done and presents a general functional view of how to accomplish it. It does not present a detailed step-by-step method for performing security evaluation. Detailed specifics of security evaluation differ widely from case to case. Any evaluation method must be adapted to meet situational needs. There is no short cut that avoids the analysis required for this situational adaptation. Detailed methods and aids such as matrices, flowcharts, and checklists are helpful in the adaptation process. This Guideline identifies such aids and methods and shows where they are best applied. However no single detailed method or aid exists that can be used universally. The value of this Guideline is in organizing and focusing the adaptation process. [NBS83] presents summaries and analyses of numerous detailed methods and aids, and is an important complement to this Guideline. [NBS83] also reaffirms an important point that bears repeating, i.e., that the fundamental requirement for successful evaluation is effective, experienced people. No methodology can offset this need.

The certification process presented here is an example. The intent is to provide guidance, not to impose a specific structure. The process is complete and generally applicable to all situations, although the appropriate level of effort varies with each situation.

Since the overall certification process described is at a functional level, it can be applied to both applications under development and those already operational. Functionally, the two situations are similar. For example, both follow the stages of figure 2-1; both include review of similar application documentation such as Functional Requirements Documents and test procedures and reports.

On the other hand, detailed evaluation methods used within the certification process differ for the two situations due to differences in both the types of data available and the organization of the work.

1. *Data Available.* Certifications performed in parallel with development are more apt to have available security-relevant products from the developers. Such products might include vulnerability analyses and security design trade-off analyses. Certifications performed on operational systems have operational documents such as problem reports, audit journal data, availability statistics and violation reports that are not available during development.

   Applications under development might be reviewed for acceptability by several offices or by a Project Steering Committee. These reviews can be used to gather evidence for certification and are discussed further in Appendix F. Operational applications have users who can be interviewed and can provide unique forms of certification evidence based on their personal experience.

2. *Organization of Work.* Certification activity during development is event-driven, being interleaved with the development process and based primarily on the availability of application documentation. Interim certification findings can be used to influence the development process itself. Certification work assignments can thus have peaks and valleys of activity as the development process occurs. Appendix F describes the interleaving of certification with development. Evaluation of an operational application can follow a more circumscribed, project-oriented structure and rely on a skill-based partitioning of the application.

2.1 Planning

The planning process is, in itself, a ''mini'' basic evaluation[4]. This is so because the plan must anticipate problem areas, needs for specialized skills, needs for support tools, and other issues that cannot be determined without insightful situation-specific analysis. Indeed, the planning process might even determine that further evaluation is not required. This might be the case, for example, if planning analysis revealed general controls to be so weak that further evaluation would be of little value. (In such cases the application still requires a security evaluation report and an accreditation decision.) Planning thus requires expertise in and knowledge of both the application and the certification process. The enlistment of external support might be required to assist in planning.

Some of the planning questions posed below are not answerable at the beginning of the effort. This is especially true of certifications of systems under development, since detailed application characteristics and much documentation are not available early in the development effort. The only approach is to consider as many issues as possible and to continue planning in parallel with evaluation activities. Planning discussion centers around four topics:

1. Initiation (getting started)
2. Analysis (determining what needs to be done)
3. Resource Definition (determining what is needed to do it)
4. Application Certification Plan (documenting the plan)

2.1.1 Initiation

For operational applications, certification and accreditation activities begin at a scheduled time, as determined by appropriate authorities such as the Accrediting Officials or the Certification Program Manager. For applications in the planning stage, certification and accreditation activities begin

[4] Two examples of ''mini'' basic evaluation questionnaires are [IBM80] and [GAO82-2].

early in the Initiation Phase of application development. The certification and accreditation program must assign responsibilities for identifying sensitive applications and for deciding which ones require certification and accreditation.

The individual responsible for managing the certification effort is referred to in this document as the Application Certification Manager. The first step upon initiation of a certification is for the Application Certification Manager to contact both the application sponsor (i.e., office responsible for the application) and the responsible Accrediting Officials. A formal introduction (e.g., via official points of contact and letters of introduction) might be desirable. The cooperation of these three individuals is crucial to the success of the effort. Together they must define the certification effort at a general level. Questions such as the following are answered.

1. What is the application involved; how sensitive is it; where are its major boundaries; where are the major anticipated problem areas; was/is security a major developmental objective; what major technological specialties are relevant?
2. How much money and time are available and appropriate for the certification; does an application risk analysis exist to help in determining appropriate certification costs?
3. Who are the responsible people; what are their roles?
4. Are there major special objectives or concerns that influence the desired quality or level of detail of the certification work?
5. Are there any special restrictions that might constrain the work?
6. Is good documentation available that describes the application and its controls; does prior review evidence exist?

It is presumed that Accrediting Officials are the primary audience for the evaluation products. Additional potential audiences are identified if this might affect the work.

It is important for the Application Certification Manager to document these issues so that a record exists of both the initiation and the initial guidance. A memorandum is suggested for this purpose, with copies sent to the Accrediting Officials and sponsoring office.

2.1.2 **Analysis**

This is the major planning activity. It is performed by the Application Certification Manager with other support as required. Analysis focuses on five major topics:

1. Applicable Policies and Requirements
2. Evidence Needed
3. Bounding and Partitioning
4. Areas of Emphasis
5. Level of Detail

Each topic is discussed below.

2.1.2.1 Applicable Policies And Requirements—Certification is the process of judging compliance with policies and requirements. It is important, therefore, that the Application Certification Manager begin by examining applicable policies and requirements since these, along with the evidential needs discussed below, represent the framework against which security evaluation for certification takes place. Applicable external policies and requirements include laws, regulations, standards, guidelines, and court decisions. Internal policies (e.g., quality assurance, test, development, and auditability standards) are also examined. Some internal policies might be very specific, addressing acceptance criteria, limits on exposures, data sensitivity, or other security-related issues. Finally, security requirements for the application itself are examined.

2.1.2.2 Evidence Needed—Evidential needs for accreditation are important in defining the specific certification evaluation methods and products required. Ideally, the evidence required for agency accreditations is standard throughout the agency and is defined in the overall agency Certification and Accreditation Program Manual (see Sec. 3.1.2). The agency's evidential accreditation requirements must then be translated to the implementation level for each particular effort. Situational variations in evidential requirements can arise for many reasons. For example, past areas of application weakness, violations, or problem reports can necessitate the collection of detailed evidence in narrow areas. Some evidence might already exist that does not need to be duplicated. The Accrediting Officials might have personal preferences for additional types of information. Planning must accommodate these situational needs while at the same time ensuring some level of standardization of certifications and accreditations within the agency.

2.1.2.3 Bounding And Partitioning—In deciding what to do, it is also necessary to decide what not to do. The Application Certification Manager must *establish boundaries* for certification. The general rule of thumb is that the certification boundaries of an application must be drawn to include all relevant facets of an application's environment, including the administrative, physical, and technical areas. Without this, certification gives an incomplete and perhaps misleading picture of application security. For example, technical controls might be excellent but worthless if administrative security is not properly defined (e.g., separation of duties) or if physical security is inadequate.

As an example, the National Aeronautics and Space Administration (NASA)[5] has determined that in most of its sensitive applications users employ the computer center as a service bureau, and control the execution of their own application software programs through remote devices. In these cases, NASA limits certification review to user data entry, application software, and user requirements and specifications for computer center support. The computer hardware, operating system, and data processing activities not under the control of application user management are not considered integral to the application and are thus not included in the application certification review. [For completeness, however, the relevance of the security of computer components outside the application (e.g., hardware, operating system) must be discussed in the evaluation report.] On the other hand, for stand-alone applications that employ a dedicated computer, NASA certification reviews include the hardware, operating system, and associated data processing activities.

As boundaries are formulated, it is important to explicitly record security assumptions that are made about areas outside the boundaries. For example, if the operating system is excluded from certification review, it should be explicitly recorded that the operating system is assumed to provide a sufficiently secure base with respect to such things as process isolation, authentication, authorization, monitoring, maintaining the integrity of security labels, and enforcing security decisions. These assumptions are made known to the Accrediting Official(s) via the security evaluation report.

Once boundaries have been established, the Application Certification Manager must decide how to *partition the work* within the boundaries. Sometimes one person has the skills and experience to perform the full evaluation. More often a team is required, due to the range of experience needed. Figure 2-2 shows a sample partitioning; most certifications do not require evaluation in all of the areas shown.

External reviews often suffice in some of these areas. For example, reviews of physical and personnel security might have been done for the organization as a whole. An internal control review for compliance with [OMB81] might exist for administrative and accounting controls. The operating system and hardware might have already been evaluated by the DoD Computer Security Center, which provides product evaluations and an Evaluated Product Listing for computer security [DoD83].

When the certification is being performed in parallel with development, different skills are applicable to the different developmental phases. Appendix F shows which skills apply in which phases.

In partitioning the work, the Application Certification Manager examines several characteristics of the application in order to estimate required numbers and skill levels of security evaluators,

[5] NASA has developed a certification program [NASA82] in parallel with the development of this Guideline.

Admin. Security	Computer Operation	Contingency Planning	Change Control	Data Entry and Output	Operating System	Communication Security
Personnel Security	Physical Security	Environmental Controls	Development Method	Application Software Controls	Data Base Management System	Hardware

Figure 2-2. *Sample partitioning of security evaluation responsibility areas for a sensitive application*

required evaluation time, and required evaluation activities. The major characteristics examined include application size, complexity, and documentation quality.

- *Size* is a critical planning factor. The larger the application or partition, the greater the required time and number of people.

- *Complexity* is based on factors such as the nature of the functions being performed, the extent to which operating system specifics need to be examined, and the clarity and level of abstraction of the languages used (whether procedural or programming). Size and complexity are assessed not just for the application as a whole, but also for each of its component parts.

- *Documentation quality* is an important consideration in planning the evaluation. There are a number of questions to ask here. Does an application flow diagram exist? Is a listing of controls available or will this information have to be gathered from application documentation? Does documentation distinguish security controls from other functions? Do functional requirements documents, system specifications, test documentation, procedure manuals, and other documents exist? Are they up to date? Are they accurate and complete? Are they understandable? Especially for requirements documents, do people agree with them?

There might be other characteristics of the application that can affect the evaluation. Examples are a distribution of functions over physically separate sites and anticipated resistance from application personnel.

2.1.2.4 Areas Of Emphasis—An evaluation must encompass the entire application, not just its major security components, since it cannot be assumed that security-relevant areas are correctly identified. The reason for this comprehensiveness is that security deficiencies can occur almost anywhere, and sometimes arise in very unlikely places. This must be balanced against the facts that (1) evaluation resources are usually very limited, and (2) some areas (e.g., functions applicable only to nonsensitive assets) warrant less detailed coverage than others (e.g., password management). What is needed is a plan that achieves the proper blend of completeness and focused emphasis.

In general, the greatest emphasis is placed on those assets, exposures, threats, and controls associated with areas of greatest expected loss or harm. Other factors are also influential. For example, less emphasis is placed on areas where flaws are believed to be well known and understood. (Nevertheless, the existence of these flaws is addressed in the evaluation findings.)

There are many factors, in addition to the Application Certification Manager's basic experience, that can influence the proper placement of emphasis. Problem areas might have been identified by prior certifications. Audit or evaluation findings, risk analysis findings, and violation reports might identify areas of weakness and help set priorities. Application personnel themselves might point out weak areas. One method [PMM80] [NBS83] uses a group of application personnel interacting via the Delphi method to identify key areas for evaluation emphasis.

2.1.2.5 Level Of Detail—Probably the single most difficult question in performing an evaluation is: How much is enough? As difficult as it may seem to answer this question generically, there is in fact a useful answer.

- For most areas of an application, a ''basic'' (i.e., high-level overview-type) evaluation is sufficient for an evaluation judgment. Since a ''basic'' evaluation is complete at the functional level, it is also the minimum necessary if cost is a limiting factor.

- Some situations warrant ''detailed'' evaluations, because of their high sensitivity or because their fundamental security safeguards are embedded deep within the computer, out of view of a high-level look.

There are a number of criteria to be taken into consideration in determining the amount of detail needed in an evaluation. In most cases the major criteria are application sensitivity, evaluation evidence, and control location. These are discussed below. Other criteria can also be influential. Examples include (1) the amount of evidential detail needed for Accrediting Official confidence, (2) application size and complexity, and (3) the amount of Application Certification Manager and security evaluator experience, since inexperienced people might require increased detail to gain acceptable confidence in the evidence they are gathering. The decision based on these criteria can apply to the application as a whole or to components within the application.

1. *Application Sensitivity.* In general, the greater the sensitivity of an application or application component, the greater the desirable evaluation detail. Major expected loss areas of highly sensitive applications almost certainly require detailed evaluation. Similarly, basic evaluations should suffice for minor expected loss areas of applications that are sensitive but not critically so. Between these extremes there is much need for judgment.

2. *Nature of Evaluation Evidence.* This is a broad criterion. It includes prior evaluation findings, prior violation/problem reports (for operational reviews), and new evidence obtained during the evaluation (for both operational and developmental reviews). The former two indicate areas of past strength and weakness, suggesting the need for less or more evaluation detail. The latter area, evidence obtained during the evaluation, might be the single most important criterion, and also results in decisions for more or less detail. For example, the planning portion of an evaluation, via its ''mini'' basic evaluation (see Section 2.1), might determine that the application has never addressed security and is in a completely insecure state. In this case, the planning process itself might suffice for an evaluation with a basic evaluation perhaps performed later, once the major problem areas have been resolved. A detailed evaluation is inappropriate in the face of gross or fundamental security inadequacies. A detailed evaluation might also be inappropriate if the planning process reveals application security safeguards to be highly effective and well managed. Judgment is needed here, but the objective is to minimize the expenditure of certification resources on applications having either highly effective or highly ineffective security safeguards. It is usually preferable to place more certification attention on intermediate cases.

   As another example, detection of a potential problem area can necessitate more detailed analysis. This might be the case if examination of the software development method finds it provided inadequate procedures for preventing and detecting errors. Even though the application security functions that were implemented seem acceptable, this finding raises the need for more detailed evaluation to provide confidence that the entire implementation can be relied upon.

3. *Control Location.* The issue here is the extent to which application security safeguards are located within the computer, as opposed to the physical and administrative environment that surrounds the computer. Several factors influencing this include the extent to which

   a. the application relies on programmed versus user control.

b. transactions are initiated externally or internally.

c. transaction records are kept externally or internally.

Auditors will recognize these factors as influences on whether an audit is performed "around" or "through" the computer [MAI76, p. 77].

Applications in which control is external are typically evaluated at the basic level. Examples include externally-controlled (1) accounts-receivable or inventory applications, (2) message processing applications, and (3) automated teller applications. Applications in which control is primarily internal require a detailed evaluation. Examples include (1) fully automated funds-disbursement and accounting applications and (2) real-time control applications (e.g., air traffic control, NASA mission, automated production).

2.1.3 **Resource Definition**

Based on the above analysis of what needs to be done in the evaluation, the Application Certification Manager plans the resources needed to accomplish the task (i.e., time, people, administrative support, and technical tools). Time estimates include not only the time required to perform the tasks, but also the time required to acquire the resources.

General administrative support needs and technical tools (discussed in Section 3.3.3) should be defined in the overall agency Certification and Accreditation Program Manual. Other related forms of general support might include copies of documents (e.g., policies, checklists), training, personnel clearances, scheduling of travel.

Typically the most difficult resource to obtain is the people. Section 1.3 discusses required skills and experience and Section 3.3.1 summarizes several staffing difficulties. Required people might include, in addition to security evaluators, consultants, technical writers, and couriers.

For all resource estimates, underlying assumptions should be listed. The assumptions consider contingencies that might affect the availability of people or other resources.

2.1.4 **Application Certification Plan**

Based on the analysis and resource definition that has taken place, it is important to now draw up and document a plan for certifying the application (the Application Certification Plan). This plan is typically issued by the Application Certification Manager and is coordinated with involved parties before its issuance. Accrediting Official approval can also be useful, depending on the extent of any support required from the Accreditor's organization, but this support should be kept to a minimum. Production of a large document should be avoided, since evaluation resources typically cannot afford this. The agency Certification and Accreditation Program Manual can be heavily referenced and generally suffices for much of the Application Certification Plan. The Plan should be followed closely unless and until unforeseen problems arise that indicate a need to revise or modify the Plan. The Plan should include scheduled opportunities for such revisions or modifications. With more experience in planning certifications and accreditations, these revisions may become less frequent.

2.1.4.1 Contents Of The Plan—Figure 2-3 shows a sample outline of the Plan. Each section of the outline is briefly described below.

1. *Executive Summary.* This is addressed to the Accrediting Officials, and includes all they need to know about the effort.

2. *Introduction.* This identifies the application (and its major boundaries), the sensitivities involved, the Accrediting Official(s), special objectives or restrictions, general schedule constraints, and other situation-specific information such as sources for specific security

1. EXECUTIVE SUMMARY

2. INTRODUCTION
   2.1 Application Background
   2.2 Scope of Certification

3. RESPONSIBILITIES
   3.1 Evaluation Team
   3.2 Other Offices

4. EVALUATION
   4.1 Security Requirements
      4.1.1 Laws, Policy, User Needs
      4.1.2 Documentation

   4.2 Evaluation Approach
      4.2.1 Basic Evaluation Tasks
      4.2.2 Detailed Evaluation Tasks

5. SCHEDULE

6. SUPPORT REQUIRED
   6.1 Administrative
   6.2 Technical

7. EVALUATION PRODUCTS

APPENDICES
A. Accreditation Statement(s)
B. Tools to support technical evaluation (e.g., checklists)

Figure 2-3. *Sample outline for an application certification plan*

policies and requirements applicable to the application, or existing security requirements documents.

3. *Responsibilities.* Organization structure and responsibilities are identified for both the evaluation team and other offices. The partitioning of evaluation work is defined. Of particular note are any specific responsibilities of application line personnel in support of the effort. The relationship of the evaluation team to other agency offices is defined.

4. *Evaluation*

   a. *Security Requirements.* This section describes the tasks necessary for obtaining a satisfactory listing of the application's security requirements. If a security requirements document was written when the application was developed, this task is simple. If no such document exists, the evaluators will need to interview users and review applicable regulations, laws, and agency policy. A risk analysis may prove helpful for this purpose.

   b. *Evaluation Approach.* This section enumerates the tasks needed to accomplish the basic evaluation and any detailed evaluation deemed necessary. The partitioning of the evaluation work is defined. The specific tasks will probably differ for different partitions of the evaluation and might also differ between operational and developmental situations, as discussed in Sec. 2.1.4.2. General topics addressed should include: (1) the areas of emphasis, (2) levels of detail, (3) specific evaluation tasks and techniques, (4) people to be interviewed, and (5) documents to be reviewed.

5. *Schedule.* The schedule includes milestones, products, assumptions, and required inputs (e.g., briefings, documentation). The timing of the milestones is based on the time estimates articulated during resource definition (see Section 2.1.3).

6. *Support Required.* Both administrative and technical (i.e., hardware/software) support requirements are listed, as is any support required from other agency offices and application line personnel.

7. *Evaluation Products.* The security evaluation report is the primary product. This section identifies any variance from the defined report and evidence found in the overall agency Certification and Accreditation Program Manual.

8. *Appendices.* A sample accreditation statement is included. It is important that the Accrediting Officials have a clear understanding, before the effort begins, of what the statement might contain so that the contents of the security evaluation report do not come as a surprise. Also included or referenced is information on methods and tools to be used during the evaluation.

2.1.4.2 Illustrative Task Structure For Evaluation—An illustrative high-level task structure is shown below. Differences between developmental and operational certifications will show up in the details of carrying out these tasks. For example, under security testing, a developmental certification will use test data only, but an operational certification will also have available journals and logs.

1. Indoctrination—briefings, tutorial overviews.

2. Security Requirements Review—list documents to be reviewed and commented upon and interviews to be performed.

3. Security Design/Operation Review—list design documents (for developmental and operational systems) and performance documents (for operational systems) to be reviewed, commented upon, and analyzed.

4. Security Testing—list documents to be reviewed and commented upon, any operational testing to be monitored, and security testing to be defined and performed.

5. Security Support—list potential tradeoff studies, detailed analysis, and other ad hoc analysis and support.

6. Report of Findings.

2.1.4.3 Initiating The Evaluation—The first step in initiating evaluation proper involves obtaining and organizing resources described in the Plan. That is, people are recruited or assigned, resources obtained, an administrative structure established, evaluation methods and tools selected, and assignments made. The central part of the evaluation work then begins.

2.2 Data Collection

Most of the work performed during an evaluation (including the planning phase) serves the purpose of data collection. Often the techniques used to collect data represent building blocks in the construction of evaluation methods. The exact nature of the data to be collected depends on the evaluation methods and tools selected. This section discusses three data collection techniques frequently used:

1. Provision by Application Management

2. Document Review

3. Interviews

Especially for the more general information required in basic evaluation, provision by application management is recommended as the best data collection technique. The reasons for this are discussed below, followed by a discussion of each technique in more detail.

In performing an evaluation, the greatest expenditure of resources occurs not in forming the judgment but in learning the characteristics of the application. There are two major aspects of learning about the application: (1) learning what it does and how it works; and (2) determining its security posture (i.e., threats, assets, exposures, controls). Both of these learning objectives can be met by document review and interviews, as discussed below. From the agency's point of view, however, document reviews and interviews can be very time consuming and consequently less cost effective data collection mechanisms.

Ideally, documentation is the best source for information about the application. Unfortunately much application documentation is of poor quality and in many cases does not exist. On the other hand, where it does exist there can be hundreds or thousands of pages of documentation associated with an application. This documentation might be vague or outdated, and often does not segregate or even explicitly identify security controls. As a learning vehicle, actual application documentation often leaves much to be desired.

Interviews also have major shortcomings. The primary one is that they often are time consuming for the amounts of information produced. A typical interview involves at least a person-day of work, including preparation and documentation time, along with the time of two interviewers and one interviewee. Frequently this cannot be justified for the amount of information obtained in a typical interview for security evaluation purposes.

The basic problem giving rise to this inefficiency is that with document reviews and interviews, the wrong people are gathering the information. The people able to gather information about an application most efficiently are those people most familiar with it, such as developers and users. The least time consuming data collection technique, then, is for application management to provide application information by tasking application developers and users to formulate and present it to the evaluation team.

Where security expertise is required, as in the preparation of security requirements, it is often best for application and certification personnel to work together. For developmental applications, the security evaluators should participate in the requirements review procedures. For operational applications which do not have explicitly expressed security requirements, application and certification personnel should work together to arrive at an accurate understanding and description of these requirements.

It is possible that the data collection process will detect evidence of fraud or crimes. Such evidence must be turned over to appropriate authorities (e.g., the OIG). Care must be taken to consult with the organization's legal staff so as not to take any inappropriate action that might, for example, impede investigation or prosecution or open oneself to legal action.

2.2.1 Provision By Application Management

As noted above, there are two major areas for data collection:

1. What does the application do and how does it work?
2. What is its security posture with respect to threats, assets, exposures, and controls?

Application management provision of this information involves the use of application personnel to provide introductory and detailed briefings and tutorials on the application and its security safeguards. It also includes the provision of *four key documents.* Ideally, these documents already exist. Typically, however, most do not and must be formulated for the certification.

- *Security Requirements*—First and foremost are the application security requirements themselves. As discussed below in Section 2.3.1, security requirements are the fundamental baseline for certification and accreditation. If an acceptable statement of requirements does not exist, it must be formulated during the certification. This is best done through a joint effort of certification and application personnel. Certification personnel are needed because typically application personnel do not have a thorough understanding of computer security, especially with respect to external policies. Application personnel are needed because certification personnel usually do not have a thorough understanding of the application, especially with respect to situational user needs and preferences.

- *Risk Analysis*—The second key document is an application risk analysis showing threats and assets [FIPS31 and FIPS65]. This is useful in validating the requirements and in defining the underlying problem to be solved. Again, where this does not exist, it is best prepared through a joint effort by certification and application personnel.

- *Application Flow Diagram*—Third is an application flow diagram showing inputs, processing steps, and outputs. Complete transaction flows must be included for important transaction types. This is critical for an understanding of the application. It is best prepared by application personnel.

- *List of Application Controls*—The final key document is a listing of application controls. Controls can be the most difficult application-specific portion of the security picture for an outsider to define, since they are so varied and situation-specific. On the other hand, this definition is not easy for insiders, either. For example, as application personnel gather this information, one common difficulty they face is the seemingly simple task of distinguishing controls (e.g., authorization mechanisms, sequence checking) from application activities subject to control (e.g., initiation, recording, transcription, calculation). A useful rule of thumb is that a control is any protective action, device, procedure, technique, or other measure that reduces exposure(s) [MAI76, p. 34].

Provision of this information by application personnel can have benefits beyond that of easing the burden of data collection. In particular, it can significantly increase the security awareness of application personnel. This increased awareness alone is a significant benefit. It can also draw the attention of certification personnel to application areas that are not well understood and that might thus warrant closer analysis.

Evaluation personnel should not accept documentation provided by application management as absolutely accurate, since application personnel might not be objective (see both the introduction to Section 1 and Section 3.2). Document reviews and interviews are useful in validating this information. Nevertheless, documentation provided by application personnel often proves to be an excellent source of information, and it has the added advantage of making the certification process as a whole less expensive for the agency.

2.2.2 Document Review

The second data collection technique discussed here is document review. Document review becomes increasingly important as evaluation attention focuses on more detailed issues.

The potential set of documents to be reviewed varies substantially in each certification, depending on evaluatior ɔbjectives and the availability and value of documentation. Appendix D presents an illustrative listing of documents that might be reviewed in a very large-scale certification effort. In general, the more detailed the document, the more reviews should concentrate on only security-relevant or sample portions of it. An example of this latter situation occurs when only sample source listings are examined to judge compliance with programming standards.

Some of the documents listed in Appendix D such as violation reports, audit journals, and operational statistics are only available in operational applications. Most are subject to review whether the application is operational or under development.

Appendix D illustrates the differing purposes that can underlie a review. It defines two types of review: critical and research/reference. Critical reviews involve an analysis for security deficiencies. Research/reference reviews help evaluators to understand application functionality and characteristics or reported shortcomings in order to better perform critical reviews. These different purposes might require separate passes through the documents. If evaluation support is being obtained externally, possible deliverable items might include written comments on documents reviewed.

2.2.3 **Interviews**

Interviews, though time consuming, can sometimes produce information not available through other means. Some guidance already exists on the planning and conduct of interviews as well as on interviewing strategies (since the way in which a question is asked can be as important as the question itself). Appendix E contains an interview procedure developed in support of the U. S. Department of Agriculture (USDA) certification program. Two points about interviews are discussed here: planning the interview and ensuring accurate information.

1. *Planning the Interview.* This must be stressed. Questions such as the following must be answered carefully.

   a. Which people should be interviewed (e.g., managers, users, developers, people from outside the agency)?

   b. What is the subject and purpose of each interview; what expertise is required of the interviewer?

   c. When, where, and under what conditions (e.g., people in attendance) do the interviews take place?

   d. What preparatory activities and materials (e.g., questionnaires, cameras) are needed?

   e. What documentation of the interview is required?

   f. What coordination is needed to arrange the interviews?

   g. Which interviews are dependent on findings from others?

   Questions to be asked during the interview should be prioritized so that important ones are answered early. Questionnaires presented to the interviewee in advance or used during the interview can be useful. At the beginning of the interview, the interviewee should be asked whether a tape recorder may be used. Tape recorders are generally not used since they can dissuade people from discussing sensitive subjects, but occasionally people prefer the recorder because of fear of misquotes. If recorders are used, notes must still be taken since people do not always speak into the microphone properly.

2. *Ensuring Accurate Information.* One purpose of a certification and accreditation program is to provide checks and balances. This purpose is not served if evaluators simply report the opinions of developers and users. Some interviewees may not know the facts and others may knowingly misrepresent them. Also, evaluators may misinterpret the answers. The issue here is information quality. The use of interviews itself, as opposed to simply requiring subjects to complete questionnaires, improves information quality since the personal interaction involved helps in interpreting meanings behind words, counteracting bias, and following leads. Beyond this, there are a number of specific interview techniques in addition to the guidance included in Appendix E that can help to improve the quality of information gathered for certification.

a. Assess subject competence and bias. The subject might not be qualified to discuss certain topics. The subject might also have opinions or vested interests that bias his/her responses.

b. Independently verify and document important facts.

c. Repeat answers to important questions so mutual understanding is ensured. Record key facts immediately, rather than entrusting them to memory. Two interviewers are needed to help ensure accuracy and reduce misinterpretations of answers.

d. Determine facts upon which subject opinions are based. The interviewer might form different conclusions.

e. Tell subjects what will be done with the information. They might as a result be more open.

f. Allow subjects to remain anonymous. They might provide more information as a result.

g. Do not place great reliance on the confidence subjects associate with their own estimates.

h. If the subject's judgment appears faulty (e.g., on threat likelihood or impact), request the subject to construct most-likely, extreme, most-costly, or other scenarios. This can change and improve the subject's opinion. The interviewer should have at hand as many examples of realistic scenarios as possible to counter subject bias, since subjects sometimes form judgments based on the ease with which they can fabricate plausible scenarios. Suggest ranges, whether quantitative (e.g., 0-10, 11-50, over 50) or linguistic (e.g., low, medium, high), to prevent the subject having to formulate precise numbers (e.g., for threat frequency, losses, error rates).

i. Return draft write-up to subjects so that they can (1) correct any errors or misinterpretations by the evaluators or (2) change anything they have said and subsequently learned to be in error.

2.3 Basic Evaluation

As described in this Guideline, the security evaluation process has two levels of detail: basic evaluation and detailed evaluation. This section discusses the former; Section 2.4 the latter. As noted in the introduction to Section 2, basic evaluation typically suffices for most aspects of an application under review, although most applications also require some detailed evaluation work in problem areas. Section 2.1.2.5 presents some criteria for helping to determine when detailed evaluation is warranted.

The general distinction between basic and detailed evaluation is that basic evaluation is primarily concerned with the overall functional security posture, not with the specific quality of individual controls. For example, basic evaluation is concerned with whether access authorization at the file level is sufficient or whether it might be required at, say, the record level. As another example, it might be concerned with whether authorization subjects must include terminals or just, say, individuals and processes. Basic evaluation is also concerned with verifying that security functions actually exist and that the implementation method is of sufficient quality to be relied upon. Detailed evaluation, on the other hand, is concerned with whether security functions work properly, satisfy performance criteria, and acceptably resist penetration.

There are four tasks in a basic evaluation:

1. security requirements evaluation (are application security requirements acceptable?)

2. security function evaluation (do application security functions satisfy the requirements?)

3. control existence determination (do the security functions exist?)

4. methodology review (does the implementation method provide assurance that security functions are acceptably implemented?)

Each task is discussed below. As noted in the introduction to Section 2, basic and detailed evaluations can be performed during application development or after an application has been in operation for a period of time. Appendix H presents a simple example of activities that might be involved in a basic evaluation using the above task organization.

2.3.1 **Security Requirements Evaluation**

The major purpose of certification is to determine whether application safeguards satisfy security requirements. This process is only meaningful if the application has well-defined security requirements. Unfortunately, most applications do not. For certification to be useful, then, the security requirements imbedded in the application must be critically examined to determine whether they are reasonable and whether they comply with federal, agency, and user requirements. The requirements in question are typically those embodied in the Project Request [FIPS64], where such a document exists. Where these requirements are not documented, they must be formulated.[6] Accurate, complete, and understandable security requirements are fundamental to certification.

In both formulating and evaluating security requirements for an application, two classes of needs are considered: policy needs and situational needs. Policy needs derive from the principles and required practices that the application is obligated to pursue, such as Federal laws, regulations, standards, and agency policies. Situational needs are those deriving from the application's characteristics and environment. To determine situational needs, four primary areas are considered: assets, threats, exposures, and controls.

1. *Assets.* What should be protected?

2. *Threats.* What are assets being protected against?

3. *Exposures.* What might happen to assets if a threat is realized?

4. *Controls.* How effective are security safeguards in reducing exposures?

These are discussed further in Section 2.4.2.1. If a risk analysis has been performed for the application or its environment, many situational security needs might already be well defined.

There is a rapidly growing body of useful guidance becoming available to assist in requirements definition and evaluation. The most directly applicable (in lieu of a detailed agency security policy) are those computer security policies, standards, and guidelines now being issued by the Federal government, such as the internal control standards mandated in [OMB81] and the NBS guidelines, standards, and other NBS publications that complement this one. For example, [FIPS73] includes a discussion of application controls. Requirements formulated in other agencies can also be useful (see Appendix B for references). One promising approach to defining requirements is use of the set of evaluation criteria formulated by the DoD Computer Security Center [DoD83]. These criteria represent a categorization of security levels for computer systems based on security functions and system quality. Still other useful tools are computer security checklists and questionnaires (e.g., [AFI79, CIC75, EAF83, FAIM, FIT78, FIT81, GAO81-2, HHS78, IBM83]). Several of these are summarized in [NBS83]. Risk analysis methods (e.g., [FIPS31, FIPS65, SDC79]) are useful

[6] In the EDP audit field, control objectives express overall application requirements. When control objectives address security, the control objectives become security requirements.

for requirements pertaining to installation and especially environmental controls. Generic papers on formulating computer security acceptance criteria and developing security standards are [NEUG82] and [KON81]. Further background material is contained in two NBS Special Publications on audit and evaluation of computer security ([NBS77] and [NBS80]). No single source provides all the questions or answers for a particular situation, but they do serve as useful judgmental aids in the evaluation process. Note that the judgments of acceptability made here and below are technical judgments and do not substitute for the overall decision made by the Accrediting Official.

2.3.2 **Security Function Evaluation**

2.3.2.1 With Defined Security Requirements—Given well-defined security requirements, function evaluation becomes the most important task in basic evaluation. It determines whether security functions (control techniques)[7] such as authentication, authorization, monitoring, security management, and security labeling [DoD83] satisfy security requirements. The primary method is simply to use the stated requirements as a checklist to follow in assessing whether they are satisfied. For example, where called for in requirements: Is individual accountability provided? Are subjects and objects identified and given security labels? Is an execute-only mode of access provided? Are all file accesses recorded? Are functions partitioned so as to provide separation of duties? Does a contingency plan exist and has it been tested [FIPS87]?

In some cases requirements specify only the need for a generic function such as authentication. In other cases the requirements call for use of a specific mechanism, such as a particular password technique. In both situations, function evaluation identifies the defined security function and examines it for acceptability.

2.3.2.2 Without Defined Security Requirements—Situations arise in which a reliable requirements baseline does not exist and it is not possible or appropriate to formulate one. These situations call for a more elaborate method for function evaluation. Most of the guidance sources discussed above under requirements evaluation are helpful in these situations. Several (e.g., [CIC75, GAO81-2, IBM80]) are structured in such a way that they might be termed as "methods" for doing this. Without a reliable requirements baseline to work from, however, it is difficult to assess control acceptability. Some controls are more important than others. Some are redundant or complementary. Some are effective while others may also be efficient. Some look effective but are not. Most are only effective if properly situated. Different controls have different purposes and are of differing quality.

One suitable "method" for those situations in which requirements are not well-defined is that in [MAI76], as summarized in [NBS83]. It examines how effectively controls counter specific threats and thereby reduce the resultant exposures. It also emphasizes the differing purposes and reliability of controls (e.g., computerized controls are more reliable) and incorporates analysis of control quality and placement. It emphasizes analysis of key controls. The emphasis on threats and exposures (though not on assets) makes the method similar to risk analysis. This is appropriate since, in lieu of well-defined requirements, a baseline is still needed against which to assess controls. Whereas risk analysis uses expected loss as a baseline, however, [MAI76] uses reduction of exposures.

2.3.2.3 Level of Detail—An important concern for function evaluation is the appropriate level of detail. The recommendation is that basic evaluations be complete (for all applicable control features) down through the functional level, where "functional level" is the logical level represented by functions as defined in (or appropriate for definition in) the Functional Requirements Document. This notion applies to both controls within the computer and physical/administrative controls external to it (although the latter might not actually be defined in a Functional Requirements Document).

[7] At the functional level, application controls would be described ideally in terms of control techniques or standards. The actual control mechanisms selected would appear at the implementation level. However, in practice, these distinctions are often blurred.

This function evaluation approach is suggested in full realization of the difficulty sometimes confronted in determining which functions to include in a Functional Requirements Document. It is also recognized that many applications do not have such documents associated with them. Furthermore, where such documents exist, they are often incomplete, forcing an evaluator to examine operating procedures, specifications, and other documents, in search of functional control techniques that should have been identified in the Functional Requirements Documents. Nevertheless, the functional level (1) is the level best suited to serve as a "security specification" in compliance with OMB A-71 TM1 (as noted in [FIPS73, p. 28]); (2) is a legitimate, commonly-used level (e.g., see [FIPS38]); and (3) can, when done with care, represent a *complete* picture of security functions and services, with respect to the environment surrounding the application. Completeness is necessary to ensure that major problem areas are not overlooked. The functional level does not include evaluation of individual mechanisms used to implement the security functions. This is not a problem, however, because even though implementation mechanisms can certainly influence security, they represent a level of detail not needed in a basic evaluation.

2.3.2.4 Security Requirements Documents—At this point it is useful to discuss security requirements documents in more depth. Typically the user's initial statement of requirements are contained in the Project Request [FIPS64]. The *Functional Requirements Document* is produced during the Definition Phase of development (see Appendix F). It identifies application modules at the functional level and includes inputs, outputs, processing requirements, and system performance requirements. Controls identified are also in terms of application modules and needs. Examples of such functions include authentication (e.g., passwords), authorization (e.g., subject/object definition and capabilities), and security monitoring as well as proper operation, performance, and (ideally) penetration resistance of these functions. FIPS PUB 73 provides guidance in preparing a "security specification" at this level [FIPS73, pp 29-30].

In contrast, controls at the *System/Subsystem Specification* level are the specific mechanisms required in providing the functions defined in the Functional Requirements Document (i.e., the "how it works" as opposed to the "what it does"). Examples include internal password encryption and software-module checksums. Program Specification controls typically include control counts, balancing, and checks for format, sequence, completeness, and validity. Some of these are also introduced at the code level along with typical code-level controls such as checks for input/output device errors.

In many cases, a *Data Requirements Document* [FIPS38] is produced during the Definition Phase, along with the Functional Requirements Document. Information in the Data Requirements Document is also assessed during function evaluation. This information might reveal such things as unacceptable flow, backup, manipulation, or aggregation of data, where these were not detected during requirements evaluation as discussed in the preceding section. While this examination of the Data Requirements Document is important, primary attention is usually focused on the Functional Requirements Document because it defines required security functions of the application. The Data Requirements Document is more concerned with the data to be processed by the functions. This is important, but usually not as important as whether the functions provide adequate security. For evaluations where the Data Requirements Document plays a major role, this task name can be changed from functional evaluation to functional and data requirements evaluation.

2.3.3 Control Existence Determination

The fact that functions are described in a document or discussed in an interview does not prove that they have been implemented. Basic evaluations require assurance that security function controls exist. The existence of most physical and administrative controls can be determined via visual inspection. For controls internal to the computer, testing is needed. Such testing does not gather significant evidence towards determining how well controls work since that is beyond the scope of a basic evaluation. The intent is simply to verify that the functions exist. On the other hand, quality must be kept in mind in the event there are fundamental shortcomings that call into question the overall effectiveness of the functions. A particularly vulnerable area here is the susceptibility of procedural controls to human errors.

Tests for control existence determination are straightforward. In many cases, a short operational demonstration suffices as shown in Appendix H. For example, the existence of a password function can be determined by attempting to use the application and verifying that a valid password is required. The existence of a grant access function can be determined by verifying that access is not allowed unless explicitly granted (e.g., by the file owner). Black box (external) testing is generally sufficient for control existence determination.

2.3.4 Methodology Review

Control existence determination provides assurance that controls exist. It says nothing about their quality. Even though this is a high-level overview-type evaluation, it is still desirable to gain some assurance that controls are acceptably implemented. The best way to do this without becoming immersed in testing or detailed analysis is to examine the methodology used to develop the application. This step applies regardless of whether the application is currently under development or has long been operational.

Methodology review contributes to a confidence judgment on the extent to which controls are reliably implemented and on the susceptibility of the application to flaws. This review is important since an unreliable development process can create flaws in the product. If review findings suggest that the implementation cannot be relied upon, detailed evaluation is typically required in order to find specific flaws. Specific flaws are far preferable as certification evidence than a simple judgment of low confidence.

Appendix F shows how security-relevant products and reviews are integrated into the development process. More extensive guidance is found in [FIPS73], which is also concerned specifically with the security of sensitive Federal government applications. Many other sources also provide guidance in proper development and reviews [FIPS101] [NBS81] [NBS82-3]. Software evaluation methods can embody and support effective development practices in addition to providing analytic support [NBS82-2]. One such methodology, software quality metrics [NBS83], might eventually be useful in automating portions of the methodology review. The areas of concern in reviewing a development methodology for certification are summarized below. Several of the areas also apply to security products obtained from vendors.

1. *Documentation.* Is there current, complete, and acceptable-quality documentation? This applies to both development and operational documentation.

2. *Objectives.* Was security explicitly stated and treated as an objective, with an appropriate amount of emphasis for the situation? Were security requirements defined?

3. *Project Control.* Was development well controlled? Were independent reviews and testing performed and did they consider security? Was an effective change control program used?

4. *Tools and Techniques.* Were structured design techniques used (e.g., modularization, formal specifications)? Were established programming practices and standards used (e.g., high order languages, structured walk-throughs)?

5. *Resources.* How experienced in security were the people who developed the application? What were the sensitivity levels or clearances associated with their positions?

2.4 Detailed Evaluation

In many cases a basic evaluation does not provide sufficient evidence for certification. Examples are cases where (1) basic evaluation reveals problems that require further analysis (2) the application has a high degree of sensitivity, or (3) primary security safeguards are embodied in detailed internal functions that are not visible or suitable for examination at the basic evaluation level. These situations require detailed evaluations to obtain additional evidence and increased confidence in evaluation judgments.

Detailed evaluations involve analysis of the *quality* of security safeguards. Primary tasks are examinations of the application from three points of view:

1. Functional Operation (Do controls function properly?)

2. Performance (Do controls satisfy performance criteria?)

3. Penetration Resistance (How readily can controls be broken or circumvented?)

These points of view are discussed at length below in Section 2.4.1. They apply to the evaluation of controls at a deeper level than appropriate for basic evaluation. Whereas the tasks in a basic evaluation are necessary for all certifications, those in detailed evaluation are performed as needed. Detailed evaluation consists of a collection of approaches. Selection of which to use depends primarily on the threats and exposures of concern, rather than on the general characteristics or overall sensitivity of the application. To illustrate, if the primary concern is to protect secrets from an external penetrator, penetration resistance is stressed. Agencies providing a critical service might stress system availability (a performance attribute) rather than functional operational or penetration resistance. An accounts-receivable application might place emphasis on functional operation. Ideally each of these ''points of view'' has a corresponding set of requirements or acceptance criteria against which to perform the evaluation [NEUG82].

If several points of view are to be employed, it may not be necessary to complete analysis in one area before beginning the next. In many cases, however, these points of view are not mutually exclusive and form a hierarchy that needs to be done sequentially (i.e., functional operation, performance, and penetration resistance—in that order). In all cases, each can be pursued to varying depths of thoroughness, depending on the perceived security problems. The utility of the three points of view is in organizing detailed evaluation work.

The final topic covered in this section is *detailed focusing*. Unlike basic evaluations, which need to be complete for all security safeguards down through the functional level, detailed evaluations can rarely be complete. There are simply too many controls and combinations of controls to examine every one in detail, except in extreme cases. Detailed evaluations need to be focused. Decisions of where to focus detailed evaluation attention can be among the most important decisions associated with an evaluation. Two strategies for such focusing are discussed below in Section 2.4.2.

2.4.1 **Three Points of View**

2.4.1.1 Functional Operation—Functional operation is the point of view most often emphasized in detailed evaluation since it assesses protection against human errors and casual attempts to misuse the application. Evaluations of functional operation assess whether controls acceptably perform their required functions. Although testing is the primary technique used in evaluating functional operation, other validation and verification techniques [NBS31] [FIPS101] must also be used, particularly to provide adequate analysis and review in early phases of the application life cycle. To the extent possible, certification requirements for testing are satisfied by the testing and verification performed routinely during development and operation. It is not practical for certification to duplicate these activities. On the other hand, it is desirable for certification needs to influence them. Where routine testing and verification does not provide sufficient assurance for certification, additional testing, focusing on security control function operation, must be added to satisfy certification needs. Tests for functional operation examine areas such as the following.

1. Control operation (e.g., do controls work?).

2. Parameter checking (e.g., are invalid or improbable parameters detected and properly handled?).

3. Common error conditions (e.g., are invalid or out-of-sequence commands detected and properly handled?).

4. Control monitoring (e.g., are security events such as errors and file accesses properly recorded; are performance measurements of characteristics such as resource utilization and response time properly recorded?)

5. Control management (e.g., do procedures for changing security tables work?).

To illustrate this testing, consider several of the tests needed to examine control operation of a password function:

1. Test whether access without a password is disallowed.

2. Test whether valid passwords are accepted and invalid passwords are rejected.

3. Test the interface between the password function and the access authorization function by testing whether access is properly allowed or disallowed. For example, verify that valid passwords allow proper access and do not allow improper access, and that invalid passwords result in proper access restriction.

4. Test whether the system responds correctly to multiple invalid passwords.

5. Test whether system-initiated reauthentication functions correctly.

Note that these tests are illustrative. Actual tests depend on the detailed characteristics of the specific function involved, and cannot be fully derived from a generic list such as this.

Functional operation includes the application's resistance to external errors. Therefore the test areas of primary interest include those interfaces across which errors might propagate:

1. man-man (e.g., operator messages)

2. man-system (e.g., commands, procedures)

3. system-system (e.g., intersystem dialogue)

4. process-system (e.g., calls)

5. process-process (e.g., interprocess calls)

Most test tools and methods are of use here, since functional operation is the application characteristic most often tested. Testing can be either external (''black box'' or acceptance testing) or internal (''white box,'' program testing, integration testing) depending upon the interfaces of concern. Testing can be performed by the evaluation team (see Section 1.3.4), by an agency test and evaluation group, by the developer, by the user, or by combinations of these groups. As noted above, to the extent possible, certification personnel rely on the evidence from normal development testing for certification evidence. One promising approach to internal testing for certification is the establishment of test ''measures of coverage'' criteria and the use of automated tools to measure actual test coverage. This is discussed in [NBS83], together with other aspects of security testing, and in [FIPS101].

When performed independently of the development team, internal testing can present major logistic problems. It can require stub and call routines, test data collection instrumentation, test data itself, and many other forms of support software. It can also require a full software development capability, tailored to the specific operating system and the particular application. The ideal solution is use of the facilities on which the application was originally developed. If this is not possible, careful planning is needed if major difficulties with internal testing are to be avoided.

Several "through the computer" audit techniques are applicable to functional operation testing. For example, the Test Deck method and Base Case System Evaluation, both of which are common forms of testing, are clearly applicable. Integrated Test Facility or Parallel Simulation techniques might also be of use in operational applications. Where financial controls are of concern, EDP audit experience can be particularly useful.

Some audit techniques are applicable to integrity issues rather than function operation. Techniques used to monitor production activity such as Transaction Selection or use of a System Control Audit Review File (SCARF) are applicable to operational audits or security monitoring. Data reliability assessment techniques (e.g., those contained in some Generalized Audit Software that foot and balance files) play an additional role in certification. As noted in Section 1.5.5, certification is, however, primarily focused on examining the procedures, not verifying the data ("substantive" testing). All of the audit techniques mentioned here are described in [IIA77-1].

Besides testing, there are other security evaluation tools and techniques that can be of use in examining functional operation. For example, software tools for program analysis [NBS83] [GAO81-2, p. 255] can be helpful in documentation analysis. Matrices as in [MAI76] can suggest ideas for test cases and scenarios. Checklists have utility in providing quick training as well as suggesting ideas for tests. This value will increase as more varied checklists become available to meet particular needs. For example, it can be useful, for purposes of reference and to ensure completeness, to have checklists of assets, exposures, policies, policy alternatives and issues, environmental characteristics, threats, threat and asset characteristics, factors influencing threat frequency, controls, control interactions, flaw categories, penetration approaches, tests, and so forth.

Formal verification is a technique that may be used during a detailed evaluation. Formal verification offers the hope of being able to mathematically "prove" that a functional design abides by a few simple security rules, and that lower levels of abstraction are consistent with the proven higher-level design. Formal verification is still primarily a research area, and is not widely used outside of some specialized DoD projects. Nevertheless, formal techniques are being used to develop and to verify the functional operation of weapons control, space-vehicle control, and other extremely critical applications. Such techniques might soon play a wider role. More research is needed, however, before formal verification can play a major role in a typical evaluation.

2.4.1.2 Performance—There is much more to the quality of safeguards than proper functional operation. A number of qualitative factors are listed under the general heading of performance, which is the second area of concern in detailed evaluation. These are availability, survivability, accuracy, response time, and throughput. They can be applied either to individual controls or to entire applications. Each is illustrated with an example.

1. *Availability.* What proportion of time is the application or control available to perform critical or full services? Availability incorporates many aspects of reliability, redundancy, and maintainability. It is often more important than accuracy. It is especially relevant to applications with denial of service exposures as primary concerns (e.g., air traffic control, automatic funds disbursement, production control). Security controls usually require higher availability than other portions of an application.

2. *Survivability.* How well does the application or control withstand major failures or natural disasters? "Withstand" includes the support of emergency operations during the failure, backup operations afterwards, and recovery actions to return to normal operation [FIPS87]. Major failures are those more severe than the minor or transient failures associated with availability. Survivability and availability overlap where failures are irreparable, as in space systems.

3. *Accuracy.* How accurate is the application or control? Accuracy encompasses the number, frequency, and significance of errors. Controls for which accuracy measures are especially

applicable are identity verification techniques (e.g., using signature, voice) and communication line error handling techniques [FIPS83]. Research in software quality metrics is applicable here.

4. *Response Time.* Are response times acceptable? Slow control response time can entice users to bypass the control. Examples of controls for which response time is critical are passwords (especially in distributed networks) and identity verification techniques. Response time can also be critical for control management, as in the dynamic modification of security tables. It is useful in evaluating response time to assess the impact of varying levels of degradation.

5. *Throughput.* Does the application or control support required usage capacities? Capacity includes the peak and average loading of such things as users and service requests. This can involve the analysis of performance ratios such as total users versus response time.

Testing is the best way to evaluate performance, with specific tests needed for each of the above factors that are of concern. A useful technique here is ''stress'' testing. This can involve using large numbers of users and requests, using large amounts of background activity, or employing maximal resources to attain conditions of operational stress. Functional operation might also be examined under these conditions, since stress loading often interferes with normal processing.

Stress testing is also used in a more directed fashion by attempting to exhaust quota limits for specific resources such as buffers, queues, tables, and ports. These resources might be external or internal to the application and might support application functions such as jobs, transactions, and sessions. This directed stress testing is especially useful in evaluating protection against denial of service threats.

2.4.1.3 Penetration Resistance—The final area of concern in detailed evaluation is penetration resistance. The task here is to assess resistance against the breaking or circumventing of controls, where resistance is the extent to which the application and controls must block or delay attacks. Cryptanalysis is an example of a technique for breaking a particular control, encryption. Creating and using a fraudulent log-on utility to discover passwords is an example of control circumvention. The nature of the evaluation activity here differs widely depending on whether the penetrators of concern are users, operators, application programmers, system programmers, managers, or external personnel. In addition, the notion of penetration resistance applies not only to attacks against data, but also to attacks against physical assets and performance.

Assessment of penetration resistance can be the most technically complex of the detailed evaluation categories. It is best done to establish confidence in security safeguards. It can also be done to find and correct flaws, although recent history has shown the inadequacy of ''find and fix'' as an approach for achieving security. In both cases it:

1. provides an assessment of an application's penetration resistance;

2. helps to determine the difficulties involved in actually exploiting flaws; and

3. provides a clear demonstration of flaw exploitability (since it might not be clear from analysis whether, say, an asynchronous timing flaw can be exploited).

It should not be inferred that this Guideline is recommending penetration testing as a standard technique. It is presented here as an optional subtask. Nevertheless, penetration resistance evaluation is different in kind from other forms of evaluation and can play an important role in certification.

The objective of penetration-resistance evaluation is to identify externally exploitable flaws in internal security functions and the interfaces to them. Following are illustrative areas for this detailed examination (taken primarily from [IBM76, p. 106]):

1. complex interfaces

2. change control process

3. limits and prohibitions
4. error handling
5. side effects
6. dependencies
7. design modifications/extensions
8. control of security descriptors
9. execution chain of security services
10. access to residual information

There are several approaches to structure software penetration resistance evaluation. These involve (1) searching for flaws that fall into certain categories or patterns [HOL74, LIN75, NEU78, WEBB76]; or (2) hypothesizing generic flaws and then determining if they exist [LIN75, WEI73]. Although these methods apply to the evaluation of software, similar approaches are available to evaluate hardware [AKE80] and physical and administrative controls.

When employed to assess complex objects such as large software operating systems, penetration-resistance evaluation can typically employ a team of two or three people for from two to four months. Beyond this time frame, there is a point of diminishing returns, since the object of the effort is not to find all flaws but to provide an assessment of the application's penetration resistance.

2.4.2 **Detailed Focusing Strategies**

It is rarely feasible or desirable, even in a detailed evaluation, to examine everything. Two strategies are presented for focusing on small portions of the security picture when evaluating from some or all of the three points of view discussed above. One is based on security relevant components and the other on situational analysis.

2.4.2.1 Security Components—This focusing strategy is based on four components relevant to ADP security: assets, exposures, threats, and controls. All of the components will have already been considered in the basic evaluation or in a risk analysis. The current activity involves a detailed view. It can use basic evaluation or risk analysis data where suitable, and extensions of such data, as needed, for the analysis reports.

The list of sample analysis reports discussed below for each component could be expanded. It illustrates that a variety of reports might be needed. The questions of how many and which types depends upon evaluation findings.

1. *Assets.* Assets are the tangible and intangible resources of an entity. The evaluation issue here is: What should be protected? It might be useful to examine assets (data, files, physical resources) in detail along with their relevant attributes (amount, value, use, characteristics). Most-likely targets can be identifed in this way. A variety of specific tasks might be needed. For example, an asset value analysis determines how the value differs among users and potential attackers; an asset exploitation analysis examines different ways to use an asset for illicit gain (e.g., as "insider" stock information).

2. *Threats.* Threats are possible events with the potential to cause loss or harm. "What are assets being protected against?" is the evaluation issue. In examining threats, it is important to distinguish among accidental, intentional, and natural threats. Intentional threats

can be the most complex. An example of an analysis task for intentional threats is to identify perpetrator classes (programmers, operators, users) based on knowledge, skills, and access privileges. The Relative Impact Measure (RIM) approach to security evaluation can be used for this purpose [NIE80]. Perpetrator motivation, resources, opportunity, and organization are all considered in such a process. An extensive list of generic threats is in [FIPS65, Appendix A].

Another useful analysis examines the factors affecting threat frequency. Threat frequency depends on such factors as (1) threat magnitudes, (2) assets and whether their loss is full or partial, (3) relevant exposures, (4) existing controls, and (5) expected gain on the part of the perpetrator.

The nature of the threats can influence evaluation methods used. For example, a standard evaluation technique is to review samples of source code to determine compliance with established programming practices and to look for security flaws. If the threat is a malicious developer, however, and the intent is to find "malicious" software, the assembled object code is reviewed rather than the source code or specifications, since the malicious steps will not be documented at the higher levels.

3. *Exposures.* Exposures are forms of possible loss or harm. Here the evaluation issue is: What might happen to assets if a threat (internal failure, human error, attack, natural disaster) is realized? Examples of exposures are disclosure violations, erroneous decisions, and fraud. [NBS83] discusses different exposure categories. An example of an exposure analysis is the examination of the impact of a particular exposure (e.g., greatly increased response time for a service, caused by the malicious actions of a competitor or disgruntled user). Much exposure analysis focuses on identifying areas where exposures are greatest. The question of which exposure types represent the areas of greatest loss or harm can have a major influence on detailed evaluation activities. For example, if integrity or accuracy is the primary concern, evaluation emphasis focuses on the basic application processing; if disclosure is the primary concern, evaluation emphasis falls on those functions and interfaces associated with disclosure protection.

4. *Controls.* Controls are measures that protect against loss or harm. The evaluation issue here is: How effective are security safeguards in reducing exposures? Evaluation tasks here often focus on controls embodied in specific application functions and procedures. Examples of evaluation tasks include control analysis (to examine a particular control in depth and determine its vulnerabilities and severity); work-factor analysis (to determine actual difficulties in exploiting control weaknesses); and countermeasure tradeoff analysis (to examine alternative ways to implement a control—this is often necessary in order to recommend corrective actions).

2.4.2.2 Situational Analysis—One forbidding and constraining aspect of computer security evaluation is the complexity of an application and its protective safeguards. This limits not only the percentage of the application that can be examined but also the degree of understanding attainable for those portions that are examined. These limitations represent an important and fundamental problem of security evaluation: How does one make a confident judgment based on incomplete information and partial understanding? A solution to this dilemma is the use of situational analysis. Two forms of situational analysis are discussed: the analysis of attack scenarios and the analysis of transaction flows. Both are used to complement the high-level "completeness" of a basic evaluation with detailed, well-understood examples and can focus on particular aspects of the application that are of concern (functional operation, performance, and/or penetration resistance).

An attack scenario is a synopsis of a projected course of events associated with the realization of a threat. It encompasses the four security components discussed above—threat, control, asset, and exposure—interwoven with the specific functions, procedures, and products of the application. An example of an attack scenario is a step-by-step description of a penetration, describing penetrator planning and activities, the vulnerability exploited, the asset involved, and the resulting exposure.

A transaction flow is a sequence of events involved in the processing of a transaction, where a transaction is typically an event or task of significance to and visible to the user. Transaction flow analysis is commonly used in EDP auditing [AAC78, IIA77-1] and is discussed in [NBS83]. If the application as a whole contains only a small set of transactions, transaction flow analysis might be a sufficient vehicle in itself for the detailed evaluation. A basic evaluation is still needed, however.

The idea underlying situational analysis is to focus attention on a manageable set of individual situations that can be carefully examined and thoroughly understood. This makes the resulting analysis more meaningful for several reasons.

1. It places threats, controls, assets, and exposures in context with respect both to each other and to application functions. This allows the evaluation to properly consider interdependencies, such as those among controls, and presents a balanced, realistic picture. If a detailed evaluation decomposes security components into constituent parts, a situational analysis pieces these together again into a coherent whole.

2. It emphasizes the objectives being served by control(s), and allows safeguards to be evaluated based on these objectives.

The increased understanding that can result from use of situational analysis, as well as its illustrative value, make it an important tool for use in conducting and presenting detailed evaluations.

2.5 Report of Findings

This section is concerned with the security evaluation report that is prepared for the Accrediting Official. The security evaluation report is the primary product of certification. It contains technical security recommendations for the application and is the main basis for the accreditation decision.

2.5.1 Integrating the Report

Figure 2-4 shows an example of how evaluation findings might be integrated into the security evaluation report. The evaluation work is partitioned into three areas, (1) application software and administrative and procedural safeguards, (2) physical security, and (3) operating systems and hardware. (Section 2.1.2.3 includes discussion of partitioning.) Evaluation needs in the operating systems and hardware area are satisfied externally, as might be the case if using a product evaluation from the DoD Computer Security Center [DoD83]. Most of the internal work is in the area of application software and administrative and procedural safeguards. Here there could be detailed evaluations of several partition areas that might have problems or high sensitivity. The detailed findings are combined with basic evaluation findings, and all of the findings are integrated into the security evaluation report. It is preferable to integrate findings from different evaluation areas into one final report rather than to deliver several security evaluation reports to the Accreditor, since the safeguards in each area can have complex interrelationships that require a technical interpretation.

2.5.2 Transmitting the Report

The security evaluation report is prepared under the direction of the Application Certification Manager, signed, dated, and delivered to the Accrediting Official(s). It might also be reviewed and approved by the overall agency Certification Program Manager to ensure compliance with agency standards. Typically there is a formal transmittal letter to the Accrediting Official(s) that

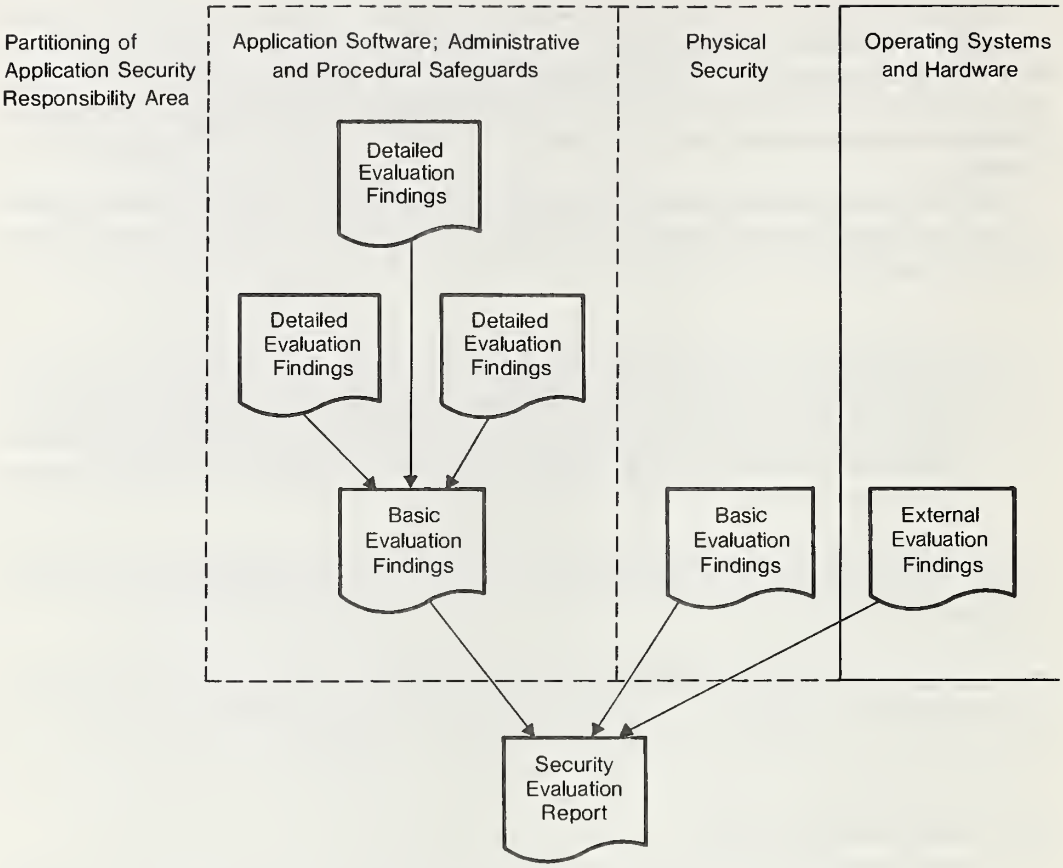

Partitioning of Application Security Responsibility Area
Application Software; Administrative and Procedural Safeguards
Physical Security
Operating Systems and Hardware
Detailed Evaluation Findings
Detailed Evaluation Findings
Detailed Evaluation Findings
Basic Evaluation Findings
Basic Evaluation Findings
External Evaluation Findings
Security Evaluation Report

Figure 2-4. *Sample documentation flow for certification findings*

describes the contents of the report and recommends signing of the accreditation statement. Figure 2-5 shows a sample transmittal letter. It includes an official certification statement in order to comply with [OMB78].

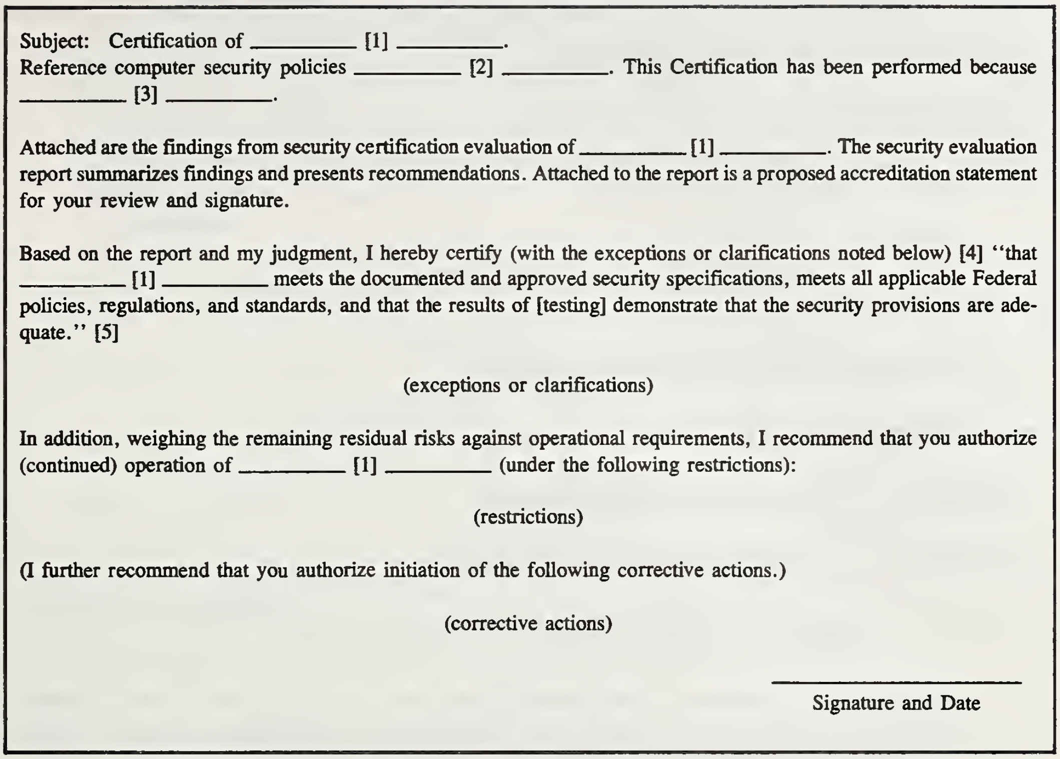
2.5.3 Sample Outline of Report

A sample outline of the security evaluation report is shown in Figure 2–6. Each section of the outline is briefly described below.

1. *Introduction and Summary.* This section briefly describes the application and summarizes evaluation findings and recommendations.

2. *Background.* This section provides contextual information for the Accrediting Official. One important item is the security standards or policies that were applied. Another is a list of the general functional characteristics of the application that generically influence its certifiability (e.g., the presence or absence of user programming). Application boundaries are defined, along with security assumptions about areas outside the boundaries.

3. *Major Findings.* The first portion of this section summarizes the controls that are in place and their general roles in protecting assets against threats and preventing exposures. This is important in maintaining perspective, and emphasizes those areas where safeguards are acceptable.



Subject: Certification of ________ [1] ________.
Reference computer security policies ________ [2] ________. This Certification has been performed because ________ [3] ________.

Attached are the findings from security certification evaluation of ________ [1] ________. The security evaluation report summarizes findings and presents recommendations. Attached to the report is a proposed accreditation statement for your review and signature.

Based on the report and my judgment, I hereby certify (with the exceptions or clarifications noted below) [4] "that ________ [1] ________ meets the documented and approved security specifications, meets all applicable Federal policies, regulations, and standards, and that the results of [testing] demonstrate that the security provisions are adequate." [5]

(exceptions or clarifications)

In addition, weighing the remaining residual risks against operational requirements, I recommend that you authorize (continued) operation of ________ [1] ________ (under the following restrictions):

(restrictions)

(I further recommend that you authorize initiation of the following corrective actions.)

(corrective actions)

____
Signature and Date

[1] Name of the application being certified.

[2] OMB A-71, TM1 and other applicable policies.

[3] Reasons include the following: (1) initial development has been completed, (2) changes have been made, (3) requirements have changed, (4) a required threshold of time has been reached, (5) a major violation has occurred, and (6) audit or evaluation findings question a previous certification.

[4] Parentheses indicate portions of the letter that are not required in some situations.

[5] Quotation from OMB A-71, TM1. The quotation marks are explanatory and, along with the editorial brackets, are not included in the actual letter.

Figure 2-5. *Sample transmittal letter for security evaluation report*

The second portion summarizes major vulnerabilities. Vulnerabilities described in the report are divided into two categories: proposed residual vulnerabilities and proposed vulnerabilities requiring correction. This format serves as both a summary of findings and a recommendation of which vulnerabilities to accept and which to correct. Authority to approve the recommendations resides with the Accrediting Official.

4. *Recommended Corrective Actions.* Here corrective actions, together with anticipated costs and impacts, are recommended and prioritized. Responsibility for making the corrections might be proposed. Also criteria must be established for evaluating the corrections. This section must be sufficiently complete to give the Accrediting Official a clear understanding of the implications of either accepting or correcting vulnerabilities.

Since sensitive applications are typically important to agency operations, most flaws will not be severe enough to remove an operational application from service although some

1. INTRODUCTION AND SUMMARY

2. BACKGROUND

3. MAJOR FINDINGS

    3.1 General Control Posture

    3.2 Vulnerabilities

4. RECOMMENDED CORRECTIVE ACTIONS

5. CERTIFICATION PROCESS

Attachment A Proposed Accreditation Statement

Attachment B (etc.) Detailed Evaluation Report(s)

Figure 2-6. *Sample outline for a security evaluation report*

restrictions may need to be implemented immediately. It is likely that a serious flaw will be severe enough to delay implementation of a change or an application under development.

Other than removing an application from service or delaying its implementation, there are many intermediate accreditation alternatives available. The most common is to withhold accreditation pending completion of corrections. Many types of operational restrictions are also possible. Examples follow.

a. Adding procedural security controls. Restricting use of the application to sites that have compensating controls.

b. Restricting the application to process only nonsensitive or minimally-sensitive data.

c. Removing especially vulnerable application functions or components. In a network environment a particularly weak node might be excluded from the network.

d. Restricting users to only those with approved access to all data being processed or to those with a sufficient ‘‘clearance’’ based on an investigation.

e. Restricting use of the application to non-critical situations where errors or failures are less severe.

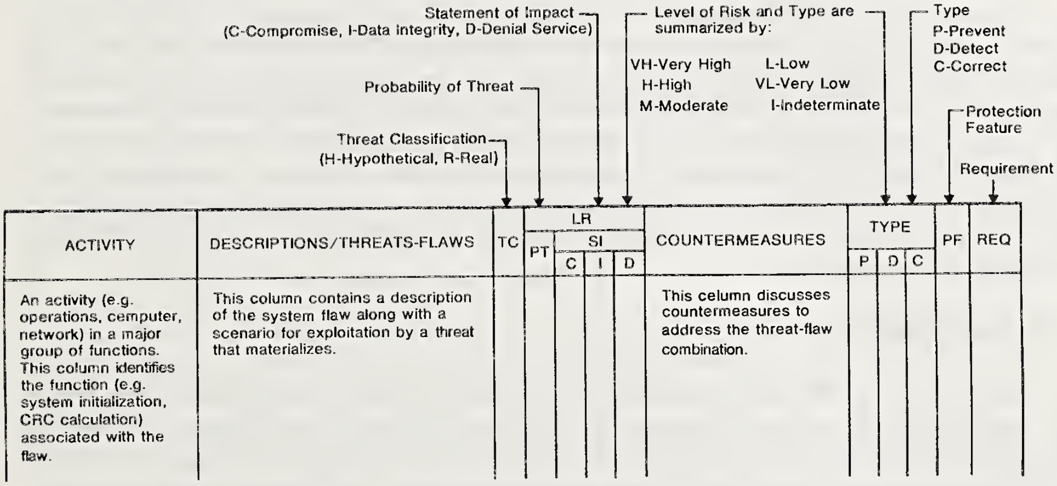
f. Removing dial-up access (thus relying more on physical security).

g. Granting conditional accreditation for a ‘‘shakedown’’ period before full trust is granted.

5. *Certification Process.* This section summarizes the work performed in the certification process. Its purpose is to enable the Accrediting Official to determine the confidence that can be placed in the findings. It might also be useful to include the Application Certification Plan as an attachment to the report.

Attachment A. Proposed Accreditation Statement. This is a critical part of the report. It summarizes recommended actions and is prepared for the Accrediting Official's signature. A sample statement is shown and discussed in Section 2.6. Judgments and recommendations embodied in the statement are subject to approval by the Accrediting Official.

Attachment B. Evaluation Report(s). These describe the full set of findings, not just major ones. It can be useful, especially if separate evaluation teams are participating, to use standard forms to present basic and detailed findings. An example of such a standard form is shown in Figure 2-7. Most columns are self-explanatory. The threat classification column permits distinction between flaws that exist and those which are suspected but for which no positive evidence can be found (e.g., malicious software, unknown operating system loopholes). Columns are available to reference applicable protection features and requirements.


Statement of Impact
(C-Compromise, I-Data Integrity, D-Denial Service)
Probability of Threat
Threat Classification
(H-Hypothetical, R-Real)
Level of Risk and Type are summarized by:
VH-Very High
H-High
M-Moderate
L-Low
VL-Very Low
I-Indeterminate
Type
P-Prevent
D-Detect
C-Correct
Protection Feature
Requirement

ACTIVITY	DESCRIPTIONS/THREATS-FLAWS	TC	LR				COUNTERMEASURES	TYPE			PF	REQ
			PT	SI				P	D	C		
				C	I	D						
An activity (e.g. operations, computer, network) in a major group of functions. This column identifies the function (e.g. system initialization, CRC calculation) associated with the flaw.	This column contains a description of the system flaw along with a scenario for exploitation by a threat that materializes.						This celumn discusses countermeasures to address the threat-flaw combination.					

Adapted from work done by System Development Corporatien fer the Defense Communications Agency.

Figure 2-7. *Sample vulnerability chart*

2.5.4 Characteristics Of The Report

Since the Accrediting Official is a high-level official, usually with a busy schedule, the security evaluation report is kept brief. The report must be accurate, meaningful, and constructive, as follows:

1. *Accurate.* All judgments must be supported. Quantitative ratings are to be avoided unless founded on demonstrably accurate data. Ratings that have a large uncertainty are often interpreted the same as accurate ones and this leads to a high potential for misunderstanding. Where ratings of some form are used, they must explicitly reflect assumptions, conditions, and variances.

2. *Meaningful.* The content and form must be understandable to the Accrediting Official. For example, it is common to separate exposures into categories (e.g., disclosure, modification, denial of service, and destruction). This breakdown might not be meaningful to a high-level manager such as the Accreditor. It might be preferable instead to orient the presentation around exposures such as fraud, competitive disadvantage, agency embarrassment, statutory sanctions, and so forth.

3. *Constructive.* Positive evidence must be summarized. Most applications are doing much more right than they are wrong. The evidence as a whole must be kept in balance. Security evaluations often report only those things that are wrong. That does not present a fair picture of all the available evidence. Similarly, recommendations must be realistic. It is not realistic to suggest that a critical application that has been running for years be shut down because of a single flaw. A more constructive suggestion is to adopt added precautionary procedures, and to begin planning on upgrades or a new version of the application.

The report is a very sensitive document; it represents a vulnerability, since it is subject to loss or abuse. Some agencies might need charters (as have been approved for criminal justice or national security data) to protect this information from Freedom of Information Act inquiries. In some cases it might be desirable to destroy the reports after they have been used (agency legal staff should be consulted here).

2.5.5 Coordinating the Report

For the report to be most effective, it typically needs to be coordinated through appropriate agency offices. (In some cases it is not desirable to coordinate the *entire* report since this might unnecessarily promulgate vulnerability information.) Offices responsible for corrective actions as well as others who might be affected are included. This increases the likelihood that recommendations will be ultimately accepted and implemented. It is possible that this coordination will result in changes to the report. This should not be viewed as threatening the report's objectivity but as helping to ensure its validity and eventual acceptance. Similar coordination is usually performed by auditors in reporting audit findings. Procedures should be established for airing and, if possible, resolving disagreements.

2.6 Accreditation

The Accrediting Official is responsible for evaluating the certification evidence, deciding on the acceptability of application security safeguards, approving corrective actions, signing the accreditation statement, and ensuring that corrective actions are acomplished. The products around which these actions are focused are the security evaluation report and the accreditation statement.

2.6.1 Using the Security Evaluation Report

The Security Evaluation Report contains evidence to support not only the evaluation findings, but also the evaluation process itself. Evaluation findings are used to assess the application while the evidence on the quality of the evaluation process can be used to assess the quality of that process. For each of the following issues the Certification Program Manager and/or Application Certification Manager might examine both the sufficiency of what was done and where improvements can be made in the evaluation activity. Some questions they might ask are:

1. Auditability. Is there a record of the evaluation that allows the work and the process to be assessed?

2. Data. How accurate are the data that were obtained?

3. Tools. Were tools effective and efficient?

4. Techniques. Were the methods used effective and efficient?

The Accrediting Official should also be able to use the report as a guide for formulating questions.

The security evaluation report is the primary evidence for the accreditation decision although there might be other evidence, such as written or verbal reports from other agency offices. The task for the Accrediting Official is to evaluate the report and its findings and recommendations. Figure 2-8 contains questions that might be asked by the Accrediting Official in assessing the report.

If the Accrediting Official decides to add security safeguards, he must approve required corrective actions and allocate sufficient resources to make the corrections. The Accreditor must also ensure that all parties understand the corrections and their roles in making them. The Accreditor might assume or delegate responsibility for follow-up examinations. It must be stressed that the identification and implementation of corrective actions are important and difficult management activities.

Resource Questions

1. How much of resources (e.g., time, money) were expanded in the evaluation?

2. Who performed the evaluation? What are their qualifications? Might there be any reasons to question their objectivity?

Process Questions

1. What technical review mechanisms were used?

2. Have the findings and recommendations been properly coordinated?

3. What major tools and techniques were used? What other experiences have there been with them? Have resources been effectively allocated to tools, analysis, and presentation of findings?

Content Questions

1. Are the findings and recommendations reasonable?

2. What are other agencies doing in similar situations? Are Federal and agency requirements applicable to this application? Are there recent or proposed policy changes that are applicable? Do agency needs override user needs? What are the penalties for not complying with policies and requirements?

3. Did the evaluation focus on those things of primary importance? What assurances are there that major problem areas have not been overlooked? Are there safeguards not considered by the evaluation activity that might influence the findings? Are the recommendations prioritized? What was the basis for prioritization?

4. Many residual vulnerabilities will exist. Have they been identified?

5. Are recommendations and judgments supported? Is the quality of supporting data shown?

Figure 2-8. *Criteria for assessing security evaluation reports*

2.6.2 The Accreditation Statement

A sample accreditation statement is shown in Figure 2-9. This format is used for reaccreditation as well as original accreditation and applies whether the application being accredited is operational or under development. Signed statements are retained as official agency records. The accreditation statement is an official document that records an explicit acceptance of responsibility for computer security. It culminates the certification and accreditation process. The true benefits

I/We have carefully examined the certification findings and recommendations documented in the [application name] security evaluation report, dated __________. Based on my/our authority and judgment, and weighing the remaining residual risks against operational requirement, I/we authorize (continued) [1] operation of [application name] (under the following restrictions).

(restrictions)

(I/We further authorize initiation of the following corrective actions.)

(corrective actions)

____
Signature(s) and Date(s)

[1] Parentheses indicate portions of the statement that are not required in some situations.

Figure 2-9. *Sample Accreditation Statement*

from certification and accreditation, however, do not derive from the statement itself. They derive rather from the checks, balances, increased security awareness, and increased management control engendered by the certification and accreditation process as a whole.

2.7 Recertification and Reaccreditation

Certification and accreditation are not permanent. As an application or its security environment changes, recertification and reaccreditation are needed to verify that security protection remains acceptable. This section addresses the scheduling and content of recertification and reaccreditation, as well as the relation between them and the change control process.

2.7.1 Scheduling

Any change or new finding that invalidates or calls into question an accreditation decision necessitates recertification and reaccreditation. Situations that give rise to this include the following:

1. *Changes to the application.* For sensitive applications, all changes large and small should be closely controlled. These various changes give rise to "levels" of recertification and reaccreditation in which, for example, small changes are controlled by a change control process while large changes may require a full recertification and reaccreditation process. Recertification and reaccreditation levels are discussed in Section 2.7.2.

2. *Changes in requirements.* This includes changes in Federal and agency security policies and in user requirements (e.g., the need to process data of a higher sensitivity). Requirements changes also include altering definitions of "good practice" as reflected in the literature or as interpreted by the courts. All of these changes raise the question of whether application safeguards satisfy the altered requirements. This question is formally addressed by recertification and reaccreditation.

3. *Passage of a time interval.* Judgments will vary on whether application or requirement changes are of sufficient scope to warrant recertification and reaccreditation. Therefore, the passage of a time interval is also used as a criterion. OMB Circular A-71 TM1 [OMB78] specifies three years as the maximum interval between recertifications. Highly sensitive applications might require annual recertification and reaccreditation. Time intervals can also be used to trigger follow-up evaluations of corrections.

4. *Occurrence of a significant violation.* A violation or incident that calls into question the findings of a prior certification may require that the application be recertified and reaccredited. If the application has never been accredited, a major violation might supply the needed impetus to do so.

5. *Audit or evaluation findings.* A recertification might be triggered based on findings deriving from an internal audit by the Office of the Inspector General (OIG), an external audit by the GAO, a spotcheck or risk analysis by the Agency ADP Security Officer, a vulnerability assessment or internal control review by an internal control committee [OMB81], or some other source.

Some of the planning issues that must be considered at the time of a recertification and reaccreditation are:

1. Should the same Accrediting Official be used?

2. Should a new Certification Plan be drawn up or the old one modified?

3. What resource allocation is needed?

As can be seen, these are extensions of the original certification and accreditation issues.

2.7.2 Recertification and Reaccreditation Levels

All applications undergo continuous change. It is not practical for the Accrediting Official to personally approve every change. On the other hand, substantive changes do require official recertification and reaccreditation. This gives rise to a need for recertification and reaccreditation "levels."

Figure 2-10 shows three illustrative levels of recertification activity. The nature of the change being made determines the level of recertification activity employed. Changes are categorized as being one of three sizes: major, intermediate, and minor. Major changes are those affecting the basic security design, such as the addition of a software access authorization package. Intermediate changes are more moderate in size and are defined in the illustration as those affecting two or more security software modules in the System Specification. Intermediate changes also include the addition or change of a major hardware component. Minor changes are those wholly within one security software module of the System Specification.

Level	Nature of Change	Accrediting Official	Certification Process
1	Major; affecting the basic security design.	Original Accrediting Official.	Full certification process: recertify entire application including portions that have not changed.
2	Intermediate; moderate changes affecting two or more security software modules as identified in the System Specification; addition or change of a major hardware component.	Intermediate sponsor management.	Partial process involving only the areas of change; formal acceptance test plan and independent testing required for security-relevant areas.
3	Minor; within one security software module and affecting no other.	Configuration Control Board	Normal change control processing; no formal acceptance test plan or independent testing required.

Figure 2-10. *Illustrative recertification and reaccreditation levels*

The organizational placement of the Accrediting Official and the elements of the certification process differ for each category of change. For major changes, the required approval authority is equivalent to that for original accreditation. The certification process also is equivalent. The entire application is recertified, not just the area of change. Intermediate changes require accreditation by an intermediate manager, with only the change itself being certified. In the example a formal acceptance test plan and independent testing are required for security-relevant areas. The lowest level of recertification in the illustration is that deriving from minor changes. These are handled through normal change control processing with no formal acceptance test plan or independent testing required. The Configuration Control Board is the accreditation authority (see Section 2.7.3). Change control is discussed below.

Typically recertification reexamines the same areas that were examined in certification. It cannot be assumed that past security assumptions remain valid. If the only prior certification was performed during development, recertification might emphasize an evaluation of operational compliance with procedures. Noncompliance is evidence that either (1) enforcement controls are lacking or (2) controls are being circumvented by users. In certifying its Uniform Payroll System, the Federal Aviation Administration uses a detailed questionnaire that distinguishes between questions applicable to certification and those applicable to recertification. The primary distinction is that the recertification questions emphasize operational compliance with procedures [FAA80].

The approach used in the figure to categorize changes is basically their size as represented in the System Specification. This is not the only possible approach to categorization and might not be the best in some situations. If a detailed risk analysis exists for the application, it might be possible to use quantitative loss estimates to identify ''major'' changes. For example, the threshold for a major change might be one involving an expected change of $1,000,000 (e.g., 1% of total assets under control) to the Annual Loss Expectancy. Such quantitative estimates are often difficult to obtain and unreliable, however, especially for software changes. The advantage of the approach shown in Figure 2-10 is that it sizes the impact of the change directly, rather than indirectly, as in a risk analysis.

2.7.3 **Change Control**

The change control (or configuration management) process is an implicit form of recertification and reaccreditation. It is required during both development and operation. For sensitive applications, change control is needed for requirements, design, program, and procedural documentation, as well as for the hardware and software itself.

The process begins during development via the establishment of ''baselines'' for the products listed above. Once a baseline is established, all changes require a formal change request and authorization. Every change is reviewed for its impact on prior certification evidence.

An entity sometimes formed to oversee change control is the Configuration Control Board (CCB). During development the CCB is a working group subsidiary to the Project Steering Committee or its equivalent. On the completion of development, CCB responsibility is typically transferred to an Operation and Maintenance (O&M) office. For sensitive applications, there should be a security representative on the CCB responsible for the following:

1. Deciding whether a change is security relevant.

2. Deciding on required security review and required levels of recertification and reaccreditation.

3. Deciding on a threshold that would trigger recertification activity.

4. Serving as technical security evaluator, especially for minor changes that might receive no other security review.

For very sensitive applications, it is appropriate to require approval and testing for all changes, however minor. A record must be kept of all changes as well as such pertinent certification evidence as test results. This record is reviewed during recertification.

3. ISSUES IN ESTABLISHING A CERTIFICATION AND ACCREDITATION PROGRAM

Section 1 addresses some of the most important management aspects of certification and accreditation: What are they, what entities are certified and accredited, who performs certification and accreditation, and when are they done? This section complements Section 1 in presenting guidance on establishing a certification and accreditation program. It is organized as follows.

3.1 Policy and Procedure Documentation. What are the primary vehicles for authorizing and defining the program?

3.2 Organization Structure. What concerns influence the organization structure for certification and accreditation?

3.3 Staffing, Training and Support. What staffing issues are confronted? What types of training and support are required?

3.1 Policy and Procedure Documentation

In order to establish a certification and accreditation program in an agency, policy and procedure guidance is needed (1) to establish official authority for the program and (2) to define the processes involved. The two documents suggested to serve these purposes are the Program Directive and the Program Manual. The former issues from the Senior Executive Officer of the agency, the latter typically from the Certification Program Manager. Subsidiary semi-autonomous components within the agency (such as the Public Health Service and the Social Security Administration) might require their own adaptations of these. A plan might also be needed to control the definition and establishment of these documents and the program itself. Such a plan is not discussed herein.

3.1.1 **Program Directive**

The Program Directive is issued under the Senior Executive Officer's signature and officially establishes the agency certification program. It is typically included as part of the directive establishing the overall agency security program and is not a stand-alone document. It contains at a minimum a program summary and an assignment of responsibility. Each of these areas is described below.

3.1.1.1 Program Summary.—The certification and accreditation program is described in general and its purpose summarized. The scope of its applicability is made clear. Reasons giving rise to the program are summarized. This can involve citing prior losses or describing attempted violations. Motivational incentives are also included. For example, one motivational approach is to include certification and accreditation activities on the critical element list against which Senior Executive Service (SES) employees are evaluated.

3.1.1.2 Responsibilities.—Major roles and responsibilities are described and assigned. These include the responsibilities of the Certification Program Manager and Major Accrediting Officials. The directive might explicitly authorize production of the Program Manual. The directive should set restrictions on delegation of accreditation authority. (Ideally it is not delegated beyond the Accrediting Official(s), except for reaccreditation.) It is important for the directive to also define the general certification support responsibilities of agency offices. For example, application, OIG, quality assurance, and test and evaluation offices must provide requested briefings, interviews, and documents and must support certification efforts in general. Potential conflicting or overlapping responsibilities with existing programs (e.g., security, internal audit) must be anticipated and addressed.

3.1.2 **Program Manual**

The Program Manual is typically issued by the Certification Program Manager (see Section 1.3.2) and serves both as a plan and as a procedures manual. It is coordinated with and reviewed by all affected parties prior to its release. Figure 3-1 shows a sample outline. The structure is similar to that of this Guideline.

The contents of the Manual depend on the specific organization and the responsibilities associated with the role of Certification Program Manager. The sample outline in Figure 3-1 assumes a detailed Manual for illustrative purposes. It should be noted that this Guideline can be used as the basis for much of the Manual. The sections of this outline are discussed below.

1. *Executive Summary.* This is addressed towards executives at all organizational levels, many of whom have little or no computer security expertise.

2. *Introduction.* The discussion of scope defines the objectives and audience of the document. The scope of actual certification activities is covered in the later sections. Definitions are either included or referenced.

3. *Summary of Computer Security Policy.* This summarizes major applicable policies. The agency computer security program must assign responsibility for updating and interpreting agency policy. If agency computer security policies are not included in the manual, they are referenced in this section, along with other applicable policies.

4. *Roles and Responsibilities.* This section defines the organization structure for certification and accreditation and assigns roles and responsibilities. It is much more detailed than the general information provided in the directive. At a minimum, the responsibilities assigned

1. EXECUTIVE SUMMARY
2. INTRODUCTION
   2.1 Scope
   2.2 Policy References
   2.3 Definitions
3. SUMMARY OF COMPUTER SECURITY POLICY (if not provided elsewhere)
4. ROLES AND RESPONSIBILITIES (including organization structure)
5. PROGRAM STRUCTURE AND CONTROL
   5.1 Applications Subject to Certification and Accreditation (initial prioritized listing, sensitivity criteria, boundary criteria, and scheduling criteria)
   5.2 Recertification and Reaccreditation Levels
6. CERTIFICATION AND ACCREDITATION TASKS
   6.1 Planning
   6.2 Data Collection
   6.3 Basic Evaluation
   6.4 Detailed Evaluation
   6.5 Report of Findings
   6.6 Accreditation Decision

APPENDICES

A. Accreditation Statement(s)

B. Tools to support technical evaluation (e.g., checklists)

Figure 3-1. *Sample outline for a certification and accreditation program manual*

include those associated in this Guideline with the roles of Accrediting Official, Certification Program Manager, Application Certification Manager, and Security Evaluator. A description of the certification support responsibilities of agency offices is also included. The section makes specific assignments whenever possible, and includes criteria for making additional assignments.

5. *Program Structure and Control.* Ideally this section includes a prioritized listing of applications requiring certification and accreditation and a schedule for planned certifications. Application boundaries are defined, along with criteria for their definition. The process and criteria used in identifying applications requiring certification and accreditation are included, as are criteria for determining evaluation depth. The section also describes the levels of recertification and reaccreditation indicating how recertifications and reaccreditations are triggered and what recertification and reaccreditation process is involved for each level.

6. *Certification and Accreditation Tasks.* This section defines the certification process, ideally defining the minimum standard that all agency certifications must meet. It includes a discussion of both the certification tasks and the administrative processing steps necessary in coordinating and performing them. The required documentation is defined and includes such information as document structure and evaluation criteria against which the documents will be judged. Steps required in coordinating findings and reaching an accreditation decision are also defined.

7. *Appendices.* These might include sample accreditation statements and descriptions of certification support tools. The tools may require procedure manuals of their own. The applicability of different tools or references for different types of training might also be discussed.

3.2 Organization Structure

There is no universally applicable best way to structure the organization of a certification and accreditation program. Each agency must define a structure that meets its own needs. Two concerns affecting this are the need for top-level management attention and the need for objectivity. Both require a balance between opposing strategies, as discussed below.

Increased top-level management attention improves a program's chances of success. This increased attention is best achieved by assigning accreditation responsibilities to higher-level people. On the other hand, the agency as a whole benefits from efficient allocation of high-level management attention to those subjects of primary importance. In agencies where expected security protection needs are low, high-level management attention to accreditation might not be warranted. For efficient use of management resources, accreditation responsibility should therefore be assigned to the lowest level of higher management that can authorize allocation of resources for security, and can accept responsibility for the entire operation.

The second concern affecting organization structure is objectivity. Objectivity is needed in the security evaluation. Since people associated with the application might have conflicting interests that encourage them to improperly downplay the importance of security (see Section 1.), objectivity is best achieved by using people who are independent of the involved application. On the other hand, independence can be costly, especially when outsiders must take the time to learn details of the application. Also, the use of application personnel as Security Evaluators, while perhaps sacrificing some objectivity, has the advantages of training them in computer security and increasing their security awareness. The best solution is often to use both internal and independent people for security evaluation.

The organization structures adopted for both the agency program as a whole and individual certification efforts depend on specifics of the agency and application. A sample organization structure supporting a certification is presented in Appendix G.

3.3 Staffing, Training, and Support

Three management issues are addressed in this section: staffing, training, and support.

3.3.1 Staffing

Certification and accreditation roles were defined and assignment criteria discussed in Section 1.3. This section summarizes several staffing issues that can present management difficulties.

1. It might be difficult to obtain sufficient resources to support the certification program. Lack of resources has been a major problem in Federal computer security programs. If this continues to be the case, most certification evaluation functions might have to be performed by line personnel rather than independently. Some agencies in this situation require line people to sign subsidiary "certification" statements attesting to the quality of their own work.
2. The need might arise for different types of specialized security evaluation support. A small permanent staff might not be able to provide this support in all cases; a large full-time staff typically cannot be afforded. Technical evaluation support must thus be acquired, either externally or internally. This may be difficult, because managers are reluctant to loan their experienced people and because transferred workers can be frustrated by temporarily working for two supervisors. Specialized experience is expensive and time-consuming to acquire externally and is of varying quality. Significant management cooperation will be needed to solve these problems.
3. The workload can be difficult to maintain at a stable level because of the varying number of ongoing certifications and the event-driven nature of developmental certifications. Flexible planning will be needed to overcome this variable workload problem.
4. The small size of a security office can make promotions difficult to obtain. As a result, people might be promoted out of the security area or might accept promotions from other organizations. Top-level management support for security career paths can help to relieve this pressure.
5. Many people do not find it rewarding to review other people's products and prefer to develop their own. Such people should not have to serve as full-time Security Evaluators. Rotating assignments will also relieve this problem.
6. Some agencies allow technical review staff to develop their skills by building software tools to aid the evaluation process. These tools can detract attention from evaluation work. A proper balance between review work and developing tools must be maintained.

3.3.2 Training

Many agencies have experienced difficulty in obtaining personnel who are trained in computer security. Without such training, technical staff members are not qualifed to perform certification activities and to make the technical judgments required in certification. Three facets of training are discussed in this section:

1. Initial general security training.
2. Application-specific training.
3. Keeping up to date.

3.3.2.1 Initial General Security Training.—Few people have computer security experience. General security training is usually required. Where classroom training is affordable, internal or consultant-sponsored classes might be available. Local colleges or universities might also offer applicable courses.

Training requires a local computer security reference library. This should contain applicable policies and general computer security references as well as a wide selection of applicable NBS computer security publications. Another important form of reference is the checklist. Several of these are required to provide the "instant" training that is sometimes necessary. Specific checklists are selected and employed based on agency needs. The following are recommended:

a. Control Objectives — 1983, EDP Auditors Foundation for Education and Research, 1983 [EAF83]. (Maps control objectives to general and detailed controls that help achieve them.)

b. Security: Checklist for Computer Center Self-Audits, AFIPS Press, 1979 [AF179]. (An excellent checklist on both technical and management issues; especially useful for hardware and software controls.)

c. Systems Auditability and Control Study, Data Processing Control Practices Report, The Institute of Internal Auditors, Inc., 1977 [IIA77-2]. (Includes a thorough overview of application controls.)

d. Evaluating Internal Controls in Computer-Based Systems, U.S. General Accounting Office, AFMD-81-76, June 1981 [GA081-2]. (Especially useful for financial and general controls.)

e. Linde, Richard R., "Operating System Penetration," *National Computer Conference Proceedings*, AFIPS Press, 1975 [LIN75]. (Includes lists of generic flaws and attacks.)

f. Neumann, Peter G., "Computer System Security Evaluation," *National Computer Conference Proceedings*, AFIPS Press, 1978 [NEU78]. (Includes lists of categories and symptoms of flaws.)

g. FitzGerald, Jerry, Internal Controls for Computerized Systems, Jerry FitzGerald & Associates, 1978 [FIT78]. (Especially useful for data communication controls.)

Multiple copies would usually be required.

3.3.2.2 Application Specific Training.—This is required upon initiation of a certification. It is generally obtained via application documentation and presentations by application personnel. In areas where an independent evaluation is not required, application training can be reduced or avoided by relying on the evidence presented by users and developers of the application. This is probably the area where the smallest amount of formal training support is available.

3.3.2.3 Keeping Up To Date. It is important for certification program participants to keep up to date. They must be aware of new policies and technology. Even more important, they must maintain an awareness of what others are doing, both for control and certification. The reason is that such practices establish the rule of thumb sometimes referred to as "due professional care." This informal, vague standard can play a major role in determining how much control and evaluation are desirable or required. The best ways to keep up to date are through courses, journals, magazines, books, and selective attendance at computer security seminars and conferences. The certification budget should be as generous as possible in all of these areas.

Specific areas to monitor include: (1) certification; (2) security programs; (3) control objectives; (4) standards and guidelines; (5) security technology; (6) test and analysis tools; and (7) evaluation methods (including VV&T, security safeguard evaluation, EDP audit, and risk analysis). Some of the more research-oriented areas to monitor are (1) acceptance criteria, (2) formal verification, (3) decision theory, (4) measures of test coverage, and (5) software quality metrics.

3.3.3 **Support**

Required administrative support and technical tools are discussed in this section.

3.3.3.1 Administrative Support.—A certification program requires the same administrative and facilities support as any other program (e.g., office space, secretarial support). It might also have some unique requirements such as:

a. Area physical access control and storage containers for sensitive data. Certification documents might be among the most sensitive in the agency.

b. Flexible office space and support facilities to support varying staff levels.

3.3.3.2 Technical Tools.—Both software and hardware might be required to support the certification program. Software tools might be needed for both development [NBS82-2] and evaluation. Such evaluation tools might include:

a. Test support software, which varies widely and include test data generators, data reduction programs, and statistical data collection routines, as well as a variety of audit-oriented software.

b. Software analysis tools, including compare utilities, complexity measures, coverage measures, path flow analyzers, and even formal verification software.

Hardware tools might include:

a. Dedicated computers
b. Terminals
c. Traffic generators
d. Hardware monitors

Finally, agency computer time must often be supplied for certification work that involves use of software and hardware.

APPENDIX A

ANNOTATED DEFINITIONS

Definitions	Remarks
Accreditation. 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 pre-specified technical requirements for achieving adequate data security. [FIPS39]	This Guideline assumes that the definition also applies more broadly to computer security in general, not just data security, and to sensitive computer applications that might not contain sensitive data.
Agency. Any executive department, military department, Government corporation, Government-controlled corporation, or other establishment in the Executive Branch of the Government (including the Executive Office of the President), or any independent regulatory agency. [PRA80]	
Asset. The tangible and intangible resources of an entity. [Adapted from WEB76]	Tangible resources include items such as physical plant, hardware, software, data, accounts receivable, cash, and personnel; intangible resources include items such as good will and competitive advantages.
Attack. The realization of a malicious-human threat. [Adapted from SDC79]	
Certification. 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 pre-specified set of security requirements. [FIPS39]	Since certification is by definition part of the accreditation process, a mandate for certification (e.g., [OMB78]) carries with it an implicit mandate for accreditation. This Guideline uses the terms computer security certification, security certification, and certification synonymously.
Control. Any protective action, device, procedure, technique, or other measure that reduces exposures. [Adapted from FIPS88, MAI76, and SDC79]	Controls can prevent, detect, or correct forms of loss or harm.
Computer Application. The use(s) for which a computer system is intentionally employed. [Adapted from SIP72]	There might be one application encompassing one or several computers or sites, although often there are several applications using a single computer.

Definitions	Remarks
Computer Security. 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.	Attacks include such things as attempts at unauthorized access and the use of ADP resources for other than authorized or intended purposes.
Computer System. An assembly of elements including at least computer hardware and usually also software, data, procedures, and people, so related as to behave as an interacting or interdependent unity. [Adapted from FIPS11, NBS80, SIP72, and WEB76]	
Exposure. A form of possible loss or harm. [Adapted from MAI76]	Examples are unauthorized disclosure, modification, destruction, and denial of service.
Internal Control Review. A detailed examination of an agency's or agency component's system of internal control to determine whether adequate control measures exist and are implemented to prevent or detect the occurrence of potential risks in a cost effective manner. [OMB81]	An agency or component-level review of accounting and administrative controls. [OMB81] requires performance of such reviews on an ongoing basis. They differ from certification reviews in their emphasis on accounting and administrative controls and their emphasis on organizational units rather than computer applications.
Risk Analysis. Risk analysis is an analysis of an organization's information resources, its existing controls, and its remaining organization and computer system vulnerabilities. It combines the loss potential for each resource or combination of resources with an estimated rate of occurrence to establish a potential level of damage in dollars or other assets. [NBS80]	
Risk Assessment. Synonymous with risk analysis.	Some agencies distinguish between risk analysis and risk assessment (e.g., [USAF82]).
Safeguard. Synonymous with control.	
Security Policy. Principles and required practices of security as pursued by an organization. [Adapted from WEB76]	
Security Requirements. Identified security needs.	These needs are expressed in Federal laws and regulations, agency standards and policies, and User's Project Requests.
Security Specifications. A detailed description of the nature and characteristics of the security functions required in an entity. [Adapted from WEB76]	This might be a stand-alone document but more likely consists of sections in the Functional and Data Requirements Documents that are described in [FIPS38].

Definitions

Remarks

Sensitive Application. 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 (e.g., automated decision-making systems). [OMB78]

Sensitive Data. Data which requires a degree of protection due to the risk and magnitude of loss or harm which could result from inadvertent or deliberate disclosure, alteration, or destruction of the data (e.g., personal data, proprietary data). [OMB78]

Sensitivity. Sensitivity is the degree of criticality of computer system components to their owners, users, or subjects and is most often established by evaluating the risk and magnitude of loss or harm that could result from improper operation or deliberate manipulation of the component. The components may be hardware, software, firmware, or data. [NBS80]

Sensitivity is discussed in Section 1.2.5.

Threat. Any circumstance with the potential to cause loss or harm. [Adapted from SDC79]

Threats arise from internal failures, human errors, attacks, and natural catastrophes.

Vulnerability. A weakness that might be exploited to cause loss or harm. [Adapted from NBS80, SDC79]

Flaws that do not increase security-relevant exposure are not relevant to security evaluation.

Vulnerability Assessment. A review of the susceptibility of an agency or program to loss or unauthorized use of resources, errors in reports and information, illegal or unethical acts, and/or adverse or unfavorable public opinion. [OMB81]

An agency or program-level risk analysis of accounting and administrative activities. [OMB81] requires performance of such reviews at least biennially. They differ in orientation from risk analysis as defined in [FIPS31] and [FIPS65] due to their emphasis on accounting and administrative activities and their emphasis on agencies or programs rather than computer applications.

APPENDIX B

COMPUTER SECURITY POLICIES AND GUIDELINES IN THE FEDERAL GOVERNMENT[1]

1. Executive Office of the President

a. Executive Order 10865, "Safeguarding Classified Information Within Industry," February 20, 1960.
b. Presidential Directive/National Security Council—24 ("PD-24"), November 16, 1977.
c. Executive Order 12333, "United States Intelligence Activities," December 4, 1981.
d. Executive Order 12356, "National Security Information," April 2, 1982.

2. Office of Management and Budget

a. OMB Circular No. A-108, "Responsibilities for the Maintenance of Records About Individuals by Federal Agencies," July 1, 1975.
b. Transmittal Memorandum No. 1 to OMB Circular A-71, "Security of Federal Automated Information Systems," July 27, 1978.
c. OMB Circular No. A-123, "Internal Control Systems," October 28, 1981.

3. General Services Administration

a. "Information Security Oversight Office Directive No. 1 Concerning National Security Information," Information Security Oversight Office, *The Federal Register*, October 5, 1978.
b. Amendment to *Federal Property Management Regulations* Part 101-35 to add 101.35.3, "Security of Federal ADP and Telecommunications Systems," (*The Federal Register*, August 11, 1980).
c. Amendment to *Federal Property Management Regulations* Subpart 101-36.7, retitled "Environmental and Physical Security," (*The Federal Register*, August 11, 1980).
d. Amendment to *Federal Procurement Regulations* to Section 1-4.1104, "Request for Procurement Action," (*The Federal Register*, October 6, 1980).
e. Amendment to *Federal Procurement Regulations* to add Section 1-4.1107-21, "Computer Security Requirements," (*The Federal Register*, October 6, 1980).

4. Office of Personnel Management

a. "Personnel Security Program for Positions Associated with Federal Computer Systems," Federal Personnel Manual (FPM) Letter 732-7, November 14, 1978. (Subsequently incorporated in the *Federal Personnel Manual* as Section 9, Subchapter 1, Chapter 732.
b. "Authorities and Guidelines for Investigations of Persons Having Access to Federal Computer Systems and Information in those Systems," Federal Personnel Manual Bulletin 732-2, January 11, 1980.

5. National Bureau of Standards

Standards

a. Federal Information Processing Standard Publication (FIPS PUB) 46, Data Encryption Standard, January 1972.
b. FIPS PUB 81, DES Modes of Operation Standard, December 1980.

[1] Adapted from [DoD80] and other sources.

Guidelines

a. FIPS PUB 31, Guidelines for Automatic Data Processing Physical Security and Risk Management, June 1974.
b. FIPS PUB 38, Guidelines for Documentation of Computer Programs and Automated Data Systems, February 1976.
c. FIPS PUB 39, Glossary for Computer Systems Security, February 1976.
d. FIPS PUB 41, Computer Security Guidelines for Implementing the Privacy Act of 1974, May 1975.
e. FIPS PUB 48, Guidelines on Evaluation of Techniques for Automated Personal Identification, April 1977.
f. FIPS PUB 64, Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase, August 1979.
g. FIPS PUB 65, Guideline for Automatic Data Processing Risk Analysis, August 1979.
h. FIPS PUB 73, Guidelines for Security of Computer Applications, June 1980.
i. FIPS PUB 74, Guidelines for Implementing and Using the NBS Data Encryption Standard, April 1981.
j. FIPS PUB 83, Guideline on User Authentication Techniques for Computer Network Access Control, September 1980.
k. FIPS PUB 87, Guidelines for ADP Contingency Planning, March 1981.
l. FIPS PUB 88, Guideline on Integrity Assurance and Control in Database Administration, August 1981.

6. General Accounting Office

a. FGMSD-76-5 "Improvements Needed in Managing Automated Decisionmaking by Computers Throughout the Federal Government," April 23, 1976.
b. FGMSD-76-27 "Computer-Related Crimes in Federal Programs," April 27, 1976.
c. FGMSD-76-40 "Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities," May 10, 1976.
d. FGMSD-77-14 "Problems Found with Government Acquisition and Use of Computers from November 1965 to December 1976," March 15, 1977.
e. LCD-77-102 "Vulnerabilities of Telecommunications Systems to Unauthorized Use," March 31, 1977.
f. FGMSD-77-32 "Computer Auditing in the Executive Departments: Not Enough is Being Done," September 28, 1977.
g. FGMSD-76-82 "New Methods Needed for Checking Payments Made by Computers," November 11, 1977.
h. LCD-76-102 "Challenges of Protecting Personal Information in an Expanding Federal Computer Environment," April 28, 1978.
i. LCD-78-123 "Automated Systems Security—Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data," January 23, 1979.
j. LCD-80-56-I "Central Agencies Compliance With OMB Circular A-71, Transmittal Memorandum No. 1," April 30, 1980.
k. LCD-81-1 "Increasing Use of Data Telecommunications Calls for Stronger Protection and Improved Economics," November 12, 1980.
l. AFMD-81-16 "Most Federal Agencies Have Done Little Planning for ADP Disasters," December 18, 1980.
m. AFMD-81-20 "Government-Wide Guidelines and Management Assistance Center Needed to Improve ADP Systems Development," February 20, 1981.
n. AFMD-81-25 "Federal Agencies' Maintenance of Computer Programs: Expensive and Undermanaged," February 26, 1981.
o. AFMD-82-7 "Federal Agencies Still Need to Develop Greater Computer Audit Capabilities," October 16, 1981.
p. Evaluating Internal Controls In Computer Based Systems—Audit Guide, June 1981.

q. Assessing Reliability of Computer Output—Audit Guide, June 1981.
r. MASAD-82-18 "Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices," April 21, 1982.

7. Congress

a. The Atomic Energy Act of 1954.
b. The Privacy Act of 1974.
c. The Freedom of Information Act of 1974.
d. The Inspector General Act of 1978.
e. The Paperwork Reduction Act of 1980.

8. Illustrative Department/Agency Level Policy Documents

a. Department of Defense

(1) DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems."
(2) DoD Manual 5200.28-M, "ADP Security Manual—Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems."
(3) Assistant Secretary of Defense Comptroller memorandum, "Interim Policy on Safeguarding Personal Information in ADP Systems."
(4) Section XIII, "Security Requirements for ADP Systems," DoD Manual 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information."
(5) DoD Manual C-5030.58-M, "Defense Special Security Communications System—Security Criteria and Telecommunications Guidance."
(6) Army Regulation 380-380, "Automated Systems Security."
(7) OPNAVINST 5239.1, "Department of the Navy Security Program for Automatic Data Processing Systems."
(8) OPNAVINST 5239.1A, "Department of the Navy ADP Security Manual."
(9) Air Force Regulation 300-8, "Automated Data Processing System (ADPS) Security Policy, Procedures, and Responsibilities."
(10) Air Force Regulation 300-13, "Safeguarding Personal Data in Automatic Data Processing Systems."
(11) DIA Regulation 50-23, "Security Requirements for Automatic Data Processing (ADP) Systems."
(12) DIA Manual 50-4, "Security of Compartmented Computer Operations."
(13) DIA Manual 50-5, "Sensitive Compartmented Information (SCI) Contractor Administrative Security—Volume II."
(14) NSA/CSS Directive 10-27, "Security Requirements for Automatic Data Processing (ADP) Systems."
(15) NSA/CSS Manual 90-4, "ADP Security Design and Operating Standards."
(16) Department of Defense Trusted Computer System Evaluation Criteria, DoD Computer Security Center, CSC-STD-001-83, August 15, 1983.
(17) Product Evaluation Bulletins, distributed by the DoD Computer Security Center.

b. Department of Agriculture

(1) Chapter 6, "ADP Security and Privacy," Departmental Information Processing Standards (DIPS) Manual.
(2) "ADP Security Handbook," USDA DIPS Manual Supplement.

c. Department of Energy

(1) DOE Order 1360.2, ''Computer Security Program for Unclassified Computer Systems.''
(2) DOE Order 5636.2, ''Security Requirements for Classified Automatic Data Processing Systems.''
(3) DOE Manual 5636.2, ''Computer Security Guidelines for Classified Automatic Data Processing Systems.''

d. Department of Health and Human Services

(1) Part 6, ''ADP Systems Security,'' Chapter 6-00, HHS ADP Systems Manual.

e. Department of Housing and Urban Development

(1) ''HUD ADP Security Policy Handbook.''

f. Department of the Interior

(1) 306 DM 7, Departmental Management Part 306 (Automatic Data Processing), Chapter 7 (ADP Security Program).
(2) ''ADP Standards Handbook'' (306 DM), Chapter 2 (ADP Security Program).

g. Department of Justice

(1) DOJ Order 2640.2, ''Automatic Data Processing (ADP) Security.''

h. Department of Transportation

(1) DOT Order 1640.7, ''Department of Transportation Automatic Data Processing Security Policy.''
(2) DOT Order 1640.8, ''Department of Transportation Automatic Data Processing Security'' (DOT ADP Security Handbook).

i. Department of the Treasury

(1) DOT Order 102-3, ''Personnel, Physical and Automatic Data Processing (ADP) Systems Security—Organization and Delegation of Authority.''
(2) Treasury Directive 10-08, Part VII, ''ADP Resource Protection.''
(3) Treasury Directive 10-08, Part VII, ''ADP Privacy Act Guidelines.''
(4) Treasury Directive 10-08, Part VII, (DRAFT) ''ADP Resource Protection Guidelines.''

j. Federal Aviation Administration

(1) ''Security Certification Guidelines for the Federal Aviation Administration's Uniform Payroll System.''

k. National Aeronautics and Space Administration

(1) NASA Management Instruction 2410.7, ''Assuring Security and Integrity of NASA Data Processing.''

l. Nuclear Regulatory Commission

(1) Part XII, ''Security of Automatic Data Processing Systems,'' Appendix to NRC Manual Chapter 2101, ''NRC Security Program.''
(2) Part XVII, ''Automated Information Systems Security Program for Sensitive Data,'' Appendix to NRC Manual Chapter 2101.

APPENDIX C

ILLUSTRATIVE SENSITIVITY CATEGORIES FOR APPLICATIONS

There are many different points of view on whether and how to categorize applications by sensitivity. Some prefer to avoid categorization, noting that all applications have some degree of sensitivity and that sensitivity is a complex, multifaceted attribute that does not lend itself to representation by simple categories. Others stress that an imperfect categorization is better than none at all. In using this Guideline, the important point is that there be agreement within the agency on which applications require certification and accreditation.

For those who prefer to establish sensitivity categories, two sample categorizations are presented here. Note that these are sensitivity categorizations for applications, not for information or personnel clearances. There is typically a correlation between these, but it cannot be assumed that a highly sensitive application contains highly sensitive information or requires highly cleared people. For example, 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 sensitive data. A sensitive application might not require cleared people if effective separation of duties removes the need for highly trusted positions.

Both categorizations are from DoD, although they might be adapted for use by non-DoD agencies. Note, for example, the GAO statement that "each executive agency head's responsibility for ensuring security of all agency information also includes information classified for purposes of national security" [GA082-1, p. 11].

The first categorization (Figure C-1) is from Army Regulation 380-380 [USA380] and has official status. The second (Figure C-2) is an unofficial categorization adapted with minor changes from [EPP80, pp. J-14, J-15]. This Guideline recommends neither approach over the other, but simply presents them for use.

A. CRITICALLY SENSITIVE (CS). A DPA which processes classified defense information or applications involving large dollar volumes of asset/resource accounting or authorization data ($10 million per annum or higher). There are four levels of critically sensitive DPA (in descending order of sensitivity):

1. Level 1 (CS1)—A DPA that processes any amount of compartmented national intelligence information or SIOP-ESI.
2. Level 2 (CS2)—A DPA that processes Top Secret information.
3. Level 3 (CS3)—A DPA that processes Secret information.
4. Level 4 (CS4)—A DPA that processes Confidential information or large dollar volumes of asset/resource accounting or authorization data.

B. HIGHLY SENSITIVE (HS). A DPA, not specifically included in A. above, which processes information requiring protection under the provisions of the Privacy Act of 1974 and/or asset/resource accounting or authorization data of moderate dollar value ($1,000,000—$10,000,000).

C. SENSITIVE. A DPA, not specifically inlcuded in A. or B. above, which processes information relating to asset/resource, proprietary or contractual information.

D. NONSENSITIVE. A DPA, not specifically included in A., B., or C. above.

Figure C-1. *Sensitivity categories for Army data processing activities (DPA)*[1]

[1] Taken from [USA380].

CRITICAL SENSITIVE. Applications shall be categorized as critical sensitive when one or more of the following criteria are met.

1. *Top Secret National Security Information.* Protection is required in the interest of national security, and the highest involved information classification designation is Top Secret.

2. *Mission Critical for Agency.* Denial of use or disablement of the application or loss, compromise, or unauthorized alteration of the data contained therein could reasonably be expected to directly and gravely degrade or jeopardize the capabilities of an agency as a whole to timely and effectively discharge its primary functions.

3. *Life Critical.* Denial of use or disablement of the application or loss, compromise, or unauthorized alteration of the data contained therein could reasonably be expected to directly and gravely jeopardize human life.

4. *Automated Decision-making Systems.* Applications, not otherwise included in the foregoing, that issue checks, requisition supplies, or perform similar asset control functions, based on programmed criteria with little human intervention, wherein the potential loss or exploitable monetary value of the assets handled could exceed $10,000,000 per year.

NONCRITICAL SENSITIVE. Applications that do not meet any of the foregoing criteria for critical sensitive shall be categorized as noncritical sensitive when one or more of the following criteria are met.

1. *Secret or Confidential National Security Information.* Protection is required in the interest of national security, and the highest involved information classification designation is either Secret or Confidential.

2. *Mission Critical for Staff Element.* Denial of use or disablement of the application or loss, compromise, or unauthorized alteration of the data contained therein could reasonably be expected to degrade or jeopardize component or major staff element capabilities to support timely and effective discharge of agency missions and functions.

3. *Privacy.* The application includes personal information requiring protection pursuant to the Privacy Act of 1974.

4. *FOIA Exemptions.* The application has been determined to be exempt from public disclosure, consistent with the requirements of the Freedom of Information Act (FOIA).

5. *Automated Decision-making Systems.* Applications, not otherwise included in the foregoing, that issue checks, requisition supplies, or perform similar asset control functions, based on programmed criteria with little human intervention, wherein the potential loss or exploitable monetary value of the assets handled could range between $1,000,000 and $10,000,000 per year.

NONSENSITIVE. All other applications that do not meet the criteria for the critical sensitive or noncritical sensitive categories as set forth above.

Figure C-2. *Illustrative sensitivity categories for applications*[1]

The two categorizations differ primarily in (1) the number of levels and sub-levels involved, (2) the treatment of classified information, and (3) the lack of explicit treatment of mission criticality in [USA380]. An area of similarity between the two is the use of the term "nonsensitive" for the lowest level. This has been criticized as implying "not sensitive" and thus susceptible to interpretation as "not needed." The Department of Commerce has defined labels for levels of record protection that avoid this problem [DoCRP1]:

1. Vital Sensitive

2. Important Sensitive

3. Useful Nonsensitive

[1] Adapted from [EPP80].

APPENDIX D

DOCUMENT REVIEW GUIDE

Purpose Code	Area/Title
	ADMINISTRATIVE
R	Organization Charts
R	Phone Book
R, C	Position Descriptions
	OPERATIONAL
R, C	Application Run Book
R, C	Application Flow Chart
R	Violation Reports
R, C	Audit Journals
R, C	Audit or Evaluation Findings
R	Problem Reports
R	Operational Statistics
R	Billing Data
R, C	Application-Specific Documents (e.g., inputs and outputs)
	REQUIREMENTS
C	Project Request
R	Feasibility Study
R	Risk Analysis
R	Cost-Benefit Analysis
C	Functional Requirements Document
R	Data Requirements Document
R	Requirements Traceability Matrix (used in DoD to correlate requirements with implementation features and tests)
	PLANS
R	Project Management Plan
C	Contingency Plan
C	Software Development/Conversion Plan
C	Security Development Plan
C	Configuration Management Plan
C	General Test Plan
R	System Integration Plan
R	Maintenance Plan
R	Data Base Management Plan
R	Integrated Logistic Support Plan
R	System Engineering Facilities Plan
	SPECIFICATIONS
C, R	System/Subsystem Specifications
C, R	Program Specifications
C, R	Data Base Specifications
C, R	Interface Specifications
C, R	Formal Specifications
R	Engineering Drawings
R, C	Human Engineering Design Approach Document
R	Engineering Change Proposals and Requests for Deviations/Waivers; Specification Change Notices
C, R	Source Listings
R	Equipment Lists
R	Floor Plan

Purpose Code	Area/Title
	MANUALS
C, R	Users Manual
C, R	System Security Manual
C, R	Computer Operators Manual
R, C	Program Maintenance Manual
R	System Manuals
	TECHNICAL ANALYSIS DOCUMENTS
R	Security Evaluation Reports (from prior certifications)
R	Risk Analysis
C	Test Procedures
C	Test Analysis Reports
R, C	Security Analysis Reports
C	Formal Verification Reports
R	Design Analysis Reports
R	Failure Mode and Effect Analysis Report
R	Reliability and Maintainability Analysis Report

KEY: C= Critical Review. Analyze for security deficiencies, whether technical, procedural, or organizational.

R= Research and Reference Review. Review to understand application functionality and characteristics or reported shortcomings in order to better perform critical reviews; use for reference purposes.

The role listed first is the highest priority role.

APPENDIX E

USDA PROCEDURE: INTERNAL CONTROL & SECURITY EVALUATION INTERVIEWS[1]

E.1 Introduction

The objective of an evaluation is for reviewers to examine an entity for the purpose of rendering an informed opinion of its state. Evaluating internal controls and computer systems security requires the talents of a number of different disciplines. Because evaluations are rare occurrences, it is not usually practical to retain a permanent staff of highly specialized technicians who only perform these reviews. A compromise is sought whereby a small number of full-time reviewers is retained (possessing the specialties most commonly used) while at the same time infrequently used technicians are matrixed into the review group as necessary. Using this approach has definite advantages: it reduces costs, exposes personnel to a wide variety of projects, and adds credibility to the reviews. On the other hand, there are also some disadvantages, the most important of which is the fact that the use of part-time reviewers requires a continuing education effort. It is certainly reasonable to expect part-time reviewers to know their specialty thoroughly, but not at all reasonable to expect them to fully understand review techniques and procedures. The purpose of this procedure, therefore, is to provide guidance to part-time reviewers in conducting interviews. Because the individual talents and skills of reviewers may vary, portions of the following material may seem obvious to some. However, to be as comprehensive as possible, such material was included.

To understand the interview process requires an understanding of the overall review process. For simplicity, it can be divided into discrete phases, each with its own duties and responsibilities. Reviewers become involved in the review during the preliminary arrangement phase and participate through the preparation of the final report.The reviewer's objective is to render an informed opinion in the final report; the objective of the information gathering phase is a means to achieve this end. Obviously, then, the information gathering phase, especially the interview portion of it, is crucial to a successful evaluation.

E.2 General Background Information

Reviewers must recognize several facts that tend to make their interviewing somewhat difficult. First, the review team is an official body, an extension of upper management. As such, it is viewed by project personnel (both agency technical area specialists and data processing personnel) with some degree of apprehension. Their current positions, past accomplishments, and perhaps even future careers may depend directly upon the project. They may not perceive the review as being in their own best interest or good for the project itself. In rare cases, project personnel may expect only negative results from an evaluation, with no positive benefit possible. Second, a variety of project personnel will be interviewed, representing a mixture of job types. As a result, reviewers will interview persons of differing levels of skills, job understanding, and intelligence. Finally, the interview itself is a form of interpersonal communication subject to the usual problems of misunderstanding between both parties.

The above factors combine in unexpected ways to complicate the job of the reviewer. It is not uncommon, for example, to interview persons who feel threatened by the evaluation, and therefore do not wish to communicate any information to "outsiders." Also, it is possible to interview persons who do not yet fully understand the project or their relation to it. On the other hand, it is entirely possible that the person being interviewed possesses the information desired, is willing and able to communicate it, but is misunderstood by the reviewer himself.

Thus, the seemingly simple interview process is, in reality, highly complex and subject to erroneous information gathering. Reviewers must always keep this in mind, and constantly strive

[1] This Appendix is taken from the certification program of the U.S. Department of Agriculture.

to obtain accurate, truthful, and relevant information about the project. To aid the process, a number of aspects relevant to interviewing are noted below.

1. **Formality**—The degree of formality varies with the position of the individual being interviewed. Generally with the higher levels of project management a more formal approach is used then with the lower levels of technical or clerical personnel. At the higher levels, formality is almost expected, but at the lower levels it may only introduce artificial barriers, hampering the free flow of information.

2. **Appointments**—In many situations project management is under time constraints that may cause conflicts with interviews. In these cases, it is advisable to arrange appointments to allow ample time to complete the entire interview without interruption. At lower levels of the project, this is usually unnecessary; it is not unreasonable for a reviewer to interview some project personnel in an impromptu manner.

3. **Personnel Selection**—There are two ways to determine who to interview: project management can choose those persons it feels can best portray an appropriate image of the project, or the review team can make its own choices. To rely solely on either method may skew the information collected, a combination of the two is far superior and produces a more balanced result.

4. **Interview Location**—The location of the interview has a direct impact upon the information gathered. It is preferable to have an assigned office borrowed from the project to conduct most of the interviews. This has several advantages—the person interviewed is more likely to be candid in a private office, reviewers do not waste time searching for the offices of others, and it is easier to control review material if it is kept in one place. However, not all interviews can take place in a fixed location; interviews of project management usually take place in their own offices.

5. **Number of Interviewers**—There is no "proper" number of reviewers to be present during an interview; individual conditions should dictate the actual number. For interviews of project management, any number seems permissible because management can be expected to be able to address a crowd, if necessary. Other members of the project team, however, may feel intimidated by the presence of too many reviewers. In these cases, at least two reviewers are recommended to help prevent communications misunderstandings between reviewers and project personnel.

6. **Project Liaison**—If the size of the project warrants, the review team should request that the project manager assign a person to act as a liaison to the review team. This greatly aids reviewers by eliminating the necessity of locating persons to interview and explaining the review process to them. Furthermore, when security walk throughs are used, it is advisable to have a project member along to assure project personnel that the review team has the authority to investigate all aspects of the project.

7. **Interview Termination**—Interviews should be terminated when all information desired is obtained (the questionnaire completed) or when it becomes obvious that the information being gathered does not justify the time being spent to acquire it (that is, the person being interviewed is either unwilling or unable to provide information.)

8. **Number of Interviews**—The number of interviews necessary to gather enough information to write the evaluation report varies from one project to another. Usually, all major operations should be investigated,—with several interviews in each functional area. However, if repeated responses to questions fail to uncover any deficiencies, the number of interviews can be reduced in that area and the time spent investigating other areas.

9. **Project Objective**—The objective of the review is to investigate and report on the project being evaluated. This is not the objective of the project itself. At times these two objectives may conflict. In such cases the daily operations of the project must take precedence over the review. Ideally, the review team should perform its function with as little disruption as possible to the project's operation and personnel.

E.3 Specific Aspects of the Interview

After all preparations have been made (background material studied, management briefing attended, appointments made, and familiarity with the questionnaire achieved) interviews can begin. From prior information gathering, a general impression of the project should already be forming. An opinion of the adequacy of the project may also be forming, but reviewers must guard against premature judgments that are unsupported by facts. Thorough study of all information may indicate several areas of concern that could be investigated more fully during interviews or by direct observation. Preparation is the key to successful evaluating; reviewers should strive to conduct interviews where they already know the answers to some of the questions asked. In this manner they can verify the information previously gathered, whether in other interviews, observations, or project documentation. The following points may expedite the interview.

Always remember that the person being interviewed may be nervous. After making initial contact try to put him at ease—introduce yourself and be sure to correctly note his name, use it often during the interview. Do not engage in trivial conversation, but do not jump immediately into minute details, either. Take the time to explain why both parties are meeting: 1) outside reviewers add objectivity and expertise to the review, 2) the agency can provide firsthand information about the status of the project. Use the first few moments to get them to talk about their job and their place in the overall project. Maintain good eye contact. If appropriate, encourage them to speak candidly by telling them that the information given will remain anonymous, not revealed to their supervisors. Try to allay any fears that the review is on a "fishing expedition," looking for only negative aspects. Explain that you will be taking notes only to ensure that the report is accurate, but do not use any type of recording device. Pay close attention to what is said, mentally sort the information to verify previously collected information and to use it to verify subsequent information. Take copious notes; all material may be needed to help compile the final report, which could be written a considerable length of time after the interview is held.

Begin filling out the questionnaire by first obtaining identification information such as the full name, title, office number and telephone number. Also, determine the length of time the individual has been in the present position in addition to previous assignments. These two seemingly unimportant facts can greatly aid the reviewer in deciding how much credence to place upon the responses. For example, if the individual has been in this present position for several years, a firm understanding of the job can be expected, with a reasonable basis for personal opinions. However, if the individual is relatively new to the position, the information given could be of little value because it may be incorrect. In such cases, it is useful to inquire about previous positions, but only if they were also with the project currently being evaluated. If so, it may be better to discuss the previous position; if not, the interview should be terminated because it serves little purpose to interview a person who has not yet settled into a new job.

Be sure to ascertain exactly where in the project the individual fits—use an organization chart, if necessary. It may be useful to obtain position descriptions prior to holding interviews so that the person's actual duties can be compared to those for which they are officially held responsible. Ask for a short explanation of duties, and note each major functional area that can be explored more fully later in the interview, but try not to interrupt this portion of the response. Determine from the duties mentioned where in the questionnaire to start asking questions—it is not unusual to skip entire sections because the individual has no working knowledge of certain areas. Do not try to rush; if additional time is needed to arrange papers to find the proper section, take it. Always retain control of the interview, and above all do not allow the individual to lead the conversation into areas of little or no interest to the evaluation.

Each time a question is asked the reviewer should follow a set procedure. Read or paraphrase the question. Explain it if the person questions some part or if the individual appears puzzled. Then stop talking and listen to the answer. Listening is the most important part of the interview; it is the reason for the interview. Oddly enough, many reviewers tend to be better talkers than listeners. Make a concerted effort to listen. If possible, do not interrupt the answer until it is complete; then if some point is unclear try to clarify it. Record the answer, either on the questionnaire, or on a note pad. Mentally verify it against previous information and remember it to verify subsequent information against it.

If any answer is unusual, unexpected, or differs from previous information, special action may be necessary. First, the importance of the discrepancy must be evaluated. If minor it can be ignored and the interview resumed without discontinuity. If a substantive disparity exists, it is a sign that problems may exist. Deviate from the questionnaire to probe into the subject as necessary—do not proceed to another topic until you are satisfied that you thoroughly understand the subject or at least the reason for the discrepancy. If unable to obtain enough information, make a note to investigate the subject in detail elsewhere. If the seriousness of the incident dictates, inform other members of the review team to be alert for further information to confirm your findings.

During interviews observe the individuals closely. If they become uncomfortable, fidget, or show signs of being excessively nervous, suspect that you are talking about a subject that, for some reason, they would rather avoid. Be extremely careful in situations such as these. There may be valid reasons for some individuals not wanting to discuss certain subjects. Decide if the subject is germane to the review—if not drop it and proceed to more important issues. If it is germane to the review, probe tactfully, with discretion. Remember that your function is not to unduly pressure project personnel. If this particular individual is reluctant to discuss an issue, it may be sufficient to simply note the topic that caused the anxiousness and investigate it further elsewhere.

A reviewer's responsibility in the interview is to obtain information about the status of the project, not to give information. Do not supply information because it might influence the responses of the individual. While speaking or listening, do not show emotion or offer judgments about the projects. Furthermore, do not indicate whether information confirms or contradicts previous sources.

After all questions are asked, it is usually a good practice to open the interview to anything the project member wishes to discuss. This could be done by saying: "We have talked about a lot of subjects. Is there anything we have not discussed that you would like to tell me at this time?" If no response is elicited, say "Is there anything this project does especially well that you would like to point out?" Reviewers should be especially attentive during this time because quite often the individual will then offer additional information, sometimes providing more useful responses than during the more structured portion of the interview.

When finished, thank the individual for contributing to the review. Also, indicate that future contact may be necessary to clarify information. Terminate the interview. As a final step, take a short time to study the questionnaire and notes. Highlight the points to be verified elsewhere, fill in any gaps that are obvious, and retain the information to be used during the writing of the evaluation report.

APPENDIX F
CERTIFICATION DURING DEVELOPMENT

Certifications performed on applications under development are interleaved with the development process. For example, the Application Certification Plan is prepared during the Initiation Phase. Security-relevant documents produced by users or developers (e.g., the Requirements Definition Document) are reviewed as they are produced. The security evaluation report and accreditation statement are produced at the conclusion of the Testing Phase.

During the development process, many agency offices have review responsibilities that can encompass security-relevant issues. Several examples follow:

a. Sponsor Management (Have user security needs been well-defined; will supporting services be adequate; does the design appear to meet user needs; are risks acceptable?)

b. Quality Assurance (Have agency quality control standards been met?)

c. Office of the Inspector General (Will the application be auditable; are internal controls adequate?)

d. Developer Management (Are security requirements feasible; can they be supported by the operating system or data base management system?)

e. Facility Management (Are security requirements feasible; will the application software, hardware, or procedures degrade overall processing or security for other facility users?)

f. General Counsel (Will the application meet legal requirements?)

Findings from this review process represent evidence that should be made available to the agency certification and accreditation program.

Certification activities can be integrated into the agency review structure for the development activity. For example, the Application Certification Manager might sit on the Project Steering Committee (PSC). A certification approach used by the Defense Communications Agency is to establish a Security Certification Working Group (SCWG) reporting to the Steering Committee. The SCWG, with representation from different agency offices, serves to centralize agency security-relevant review in making decisions on security matters.

Table F-1 shows the interleaving of certification and development activities. The table identifies (1) the purpose of each developmental phase and the tasks it entails, (2) the skills required for Security Evaluation personnel who review the products of that phase, and (3) the documentation produced during each phase. Security tasks and documents are not segregated because essentially all have security relevance. All documents, for example, include security sections or (in the case of programs) have security manifestations. Several key security documents are underlined to highlight their location. Similar tables have been developed by some agencies to meet their specific needs (e.g., [USAF82]). [FIPS73] also discusses security concerns that must be dealt with at each stage of development. Certification and accreditation needs must especially be considered in the validation, verification, and testing program employed throughout development [FIPS101].

Table F-1. Integration of certification with development[1]

	Purpose and tasks	*Security evaluator skills*	*Documentation*
INITIATION PHASE (Initial User Definition)	Determine what's being done, what needs to be done; understand problem; define scope, objectives, and operating environment; define requirements (functional, performance, methodological) and acceptance criteria.	Analysts who specialize in the application type; computer security generalists; people who understand the capabilities of the VV&T activity.[2]	Variable but typically: requirements survey; *risk analysis.* Final document: project request or technical portion of Request for Proposal (RFP).
(Evaluation and Initiation)	Perform comprehensive study of technical, economic, operational feasibility; perform cost-benefit analysis; analyze general design approaches; plan development and certification. Final package reviewed by all concerned with management decision of whether to continue. For external procurements, RFP issued, proposals evaluated, winner(s) selected.	Same as above.	Feasibility study; Cost/benefit analysis; development plan (including test plan and *application certification plan).* For external procurements, final RFP, proposals, contract(s).
DEFINITION PHASE	Translate the user requirements into detailed functional requirements and a functional architecture defining operating environment, functional modules, inputs, outputs, processing requirements, and system performance requirements (as needed to meet user performance requirements); define data requirements; complete a general top-level design; define functional interfaces (man/machine, system/system, function/function); identify equipment required; plan development activities.	Analysts; designers; engineers; VV&T specialists.	Functional requirements document; data requirements document; detailed development plan (including methodology standards); configuration management plan; acceptance test plan.
DESIGN PHASE	Design the system to meet functional requirements; divide functional modules into program modules identifying inputs, processing, and outputs of each; define control and data structures and protocols; specify interfaces in detail. Several design levels are usually needed. Prepare program specifications for modules identified in the system/subsystem specifications; prepare data base specifications; begin preparation of test procedures.	Designers; programmers; VV&T specialists.	System/subsystem specifications; program specifications; data base specifications.

Table F-1. Integration of certification with development[1]—(Continued)

	Purpose and tasks	*Security evaluator skills*	*Documentation*
PROGRAMMING PHASE	Obtain required hardware; write, test, and debug programs; prepare manuals; complete test procedures.	Programmers: analysts (for reviewing manuals); engineers (to review hardware installation); VV&T specialists.	Programs; user, operation, and maintenance manuals; test procedures; security manual (if appropriate).
TESTING PHASE	Perform integration and acceptance testing; train users and operators; install in the operational environments and adapt to each as needed; convert the data base; test in the operational environment.	Application analysts; testers; programmers; penetration specialists; VV&T specialists.	Test reports; *security evaluation report; accreditation statement.*

1. Adapted from [FIPS38, FIPS64, GAO81-1].

2. For details on VV&T and application development, see [FIPS101].

APPENDIX G
SAMPLE ORGANIZATION STRUCTURE FOR CERTIFICATION

Agencies with high levels of computer security risk might warrant certification programs with high degrees of both top-level management attention and security evaluator independence. These might be similar organizationally to Office of the Inspector General (OIG) audit programs. Most agencies, however, should probably place their certification programs at lower levels and, for evaluation work, rely more on people associated with the involved application rather than completely on independent people. A hypothetical illustration of this more typical organization structure is shown in Figure G-1. The figure shows the Assistant Secretariat for Administration within a large agency.

The Certification Program Manager is located in the ADP Plans and Policy Division of the Office of Organization and Management Information. Working for him or her is a small staff of technical managers who serve as Application Certification Managers for individual certification efforts that arise. The Certification Program Manager in this agency plays an active role in overseeing certifications throughout the agency. His responsibilities are as follows:

a. Assist in the development of the agency Certification and Accreditation Program Directive.

b. Develop and coordinate the agency Certification and Accreditation Program Manual; ensure it meets all applicable requirements; make changes as required.

c. Provide certification and accreditation support and advice to the Senior Executive Officer and Accrediting Officials as required.

d. Review and approve the Certification and Accreditation Program Manuals of subsidiary components.

e. Initiate application certifications; assign the Application Certification Managers.

f. Monitor and evaluate the individual application certifications; approvė Application Certification Plans.

g. Monitor recertification and reaccreditation activities; ensure that they are performed when required.

h. Maintain centralized records on agency certifications and accreditations.

i. Periodically report to management on program status.

The responsibilities of the Application Certification Managers are as follows:

a. Develop the Application Certification Plan for a certification effort.

b. Coordinate the procurement of internal and external (i.e., to the agency) security evaluation support.

c. Manage the security evaluation.

d. Produce the security evaluation report(s).

e. Periodically report to management on certification status.

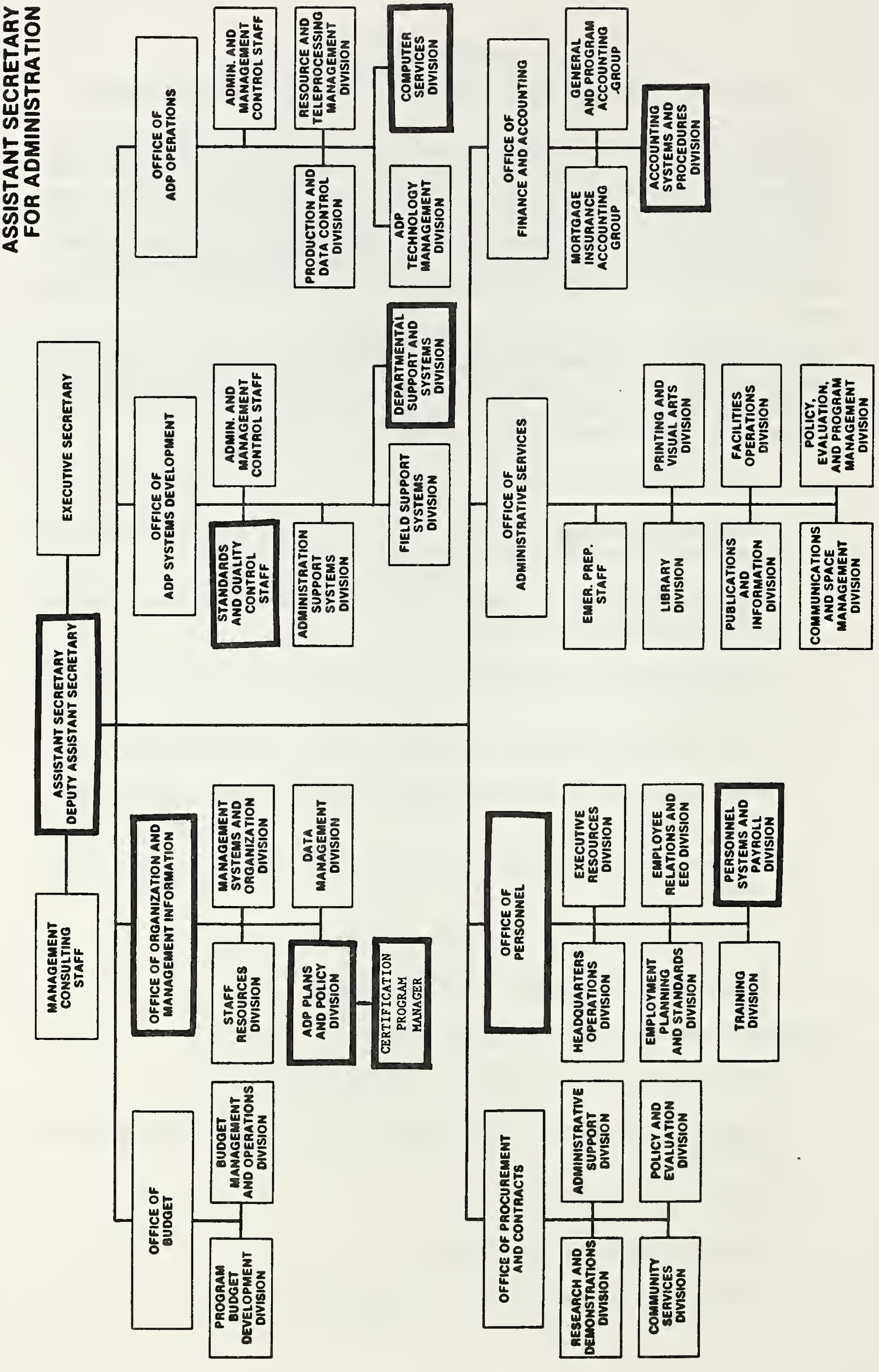

ASSISTANT SECRETARY FOR ADMINISTRATION
MANAGEMENT CONSULTING STAFF
ASSISTANT SECRETARY DEPUTY ASSISTANT SECRETARY
EXECUTIVE SECRETARY
OFFICE OF BUDGET
PROGRAM BUDGET DEVELOPMENT DIVISION
BUDGET MANAGEMENT AND OPERATIONS DIVISION
OFFICE OF ORGANIZATION AND MANAGEMENT INFORMATION
STAFF RESOURCES DIVISION
MANAGEMENT SYSTEMS AND ORGANIZATION DIVISION
ADP PLANS AND POLICY DIVISION
DATA MANAGEMENT DIVISION
CERTIFICATION PROGRAM MANAGER
OFFICE OF ADP SYSTEMS DEVELOPMENT
STANDARDS AND QUALITY CONTROL STAFF
ADMIN. AND MANAGEMENT CONTROL STAFF
ADMINISTRATION SUPPORT SYSTEMS DIVISION
FIELD SUPPORT SYSTEMS DIVISION
DEPARTMENTAL SUPPORT AND SYSTEMS DIVISION
OFFICE OF ADP OPERATIONS
ADMIN. AND MANAGEMENT CONTROL STAFF
PRODUCTION AND DATA CONTROL DIVISION
RESOURCE AND TELEPROCESSING MANAGEMENT DIVISION
ADP TECHNOLOGY MANAGEMENT DIVISION
COMPUTER SERVICES DIVISION
OFFICE OF PROCUREMENT AND CONTRACTS
RESEARCH AND DEMONSTRATIONS DIVISION
ADMINISTRATIVE SUPPORT DIVISION
COMMUNITY SERVICES DIVISION
POLICY AND EVALUATION DIVISION
OFFICE OF PERSONNEL
HEADQUARTERS OPERATIONS DIVISION
EXECUTIVE RESOURCES DIVISION
EMPLOYMENT PLANNING AND STANDARDS DIVISION
EMPLOYEE RELATIONS AND EEO DIVISION
TRAINING DIVISION
PERSONNEL SYSTEMS AND PAYROLL DIVISION
OFFICE OF ADMINISTRATIVE SERVICES
EMER. PREP. STAFF
LIBRARY DIVISION
PRINTING AND VISUAL ARTS DIVISION
PUBLICATIONS AND INFORMATION DIVISION
FACILITIES OPERATIONS DIVISION
COMMUNICATIONS AND SPACE MANAGEMENT DIVISION
POLICY, EVALUATION, AND PROGRAM MANAGEMENT DIVISION
OFFICE OF FINANCE AND ACCOUNTING
MORTGAGE INSURANCE ACCOUNTING GROUP
GENERAL AND PROGRAM ACCOUNTING GROUP
ACCOUNTING SYSTEMS AND PROCEDURES DIVISION

Figure G-1. *Illustrative organization structure*

If this were a small organization, the Certification Program Manager might also serve as Application Certification Manager for individual certifications.

Now let us assume the Personnel Systems and Payroll Division of the Office of Personnel is sponsoring the development of a new Automated Personnel Records System. Development is being done by the Departmental Support and Systems Division within the Office of ADP Systems Development.

The Certification Program Manager becomes officially involved when the Project Request Document for the new system has been prepared by the Office of Personnel. The Certification Program Manager coordinates with his division and office managers and the Office of Personnel to determine whether certification and accreditation are required and, if so, who should be the Accrediting Official. In this case certification and accreditation are deemed necessary and, because of the pervasive impact of the new system, the Assistant Secretary is identified as the appropriate authority. This proposed placement is coordinated with the Assistant Secretary to obtain his or her approval.

At this point the Certification Program Manager officially appoints from within his office an Application Certification Manager to manage the effort. The Application Certification Manager prepares an Application Certification Plan and has it approved by the Certification Program Manager and his division and office managers, the Office of Personnel, and the Assistant Secretary.

Technical security evaluation of the evolving Automated Personnel Records System is performed by diverse agency offices (as a slight extension of their normal review roles) and coordinated by the Application Certification Manager. Offices performing technical review roles relevant to the certification effort include the following:

a. Departmental Support and Systems Division
b. Personnel Systems and Payroll Division
c. Standards and Quality Control Staff
d. Computer Services Division
e. Accounting Systems and Procedures Division
f. Office of the Inspector General
g. General Counsel

The latter two are not shown on the organization chart because they are outside the Assistant Secretariat for Administration. Technical people assigned full-time to the Certification Program Management or Agency ADP Security offices might also support the certification.

On completion of the effort, the Application Certification Manager oversees the production of the security evaluation report, coordinates it with involved offices, and forwards it through channels to the Assistant Secretary. The Assistant Secretary signs the accreditation statement and assigns responsibilities for corrections and follow-up actions. The Certification Program Manager maintains a copy of the accreditation statement on file.

In this agency, it happens that the Certification Program Manager also serves as the Agency ADP Security Officer. In this role, he performs several tasks that are relevant to the certification and accreditation program:

a. Defines agency computer security policies.
b. Reviews and approves the security-relevant policies and standards of various agency offices.
c. Assists in developing security requirements and in security testing.
d. Performs security "spot checks" at irregular intervals.
e. Investigates security breaches.
f. Maintains records of security problems and violations.

This example illustrates the responsibilities that might be associated with an agency certification program and shows how they can be assigned.

APPENDIX H

BASIC EVALUATION EXAMPLE

H.1 Introduction

This appendix presents a simple example of activities that might be involved in a basic evaluation. It is oriented around a simplified set of requirements for access authorization. In an actual basic evaluation, all security requirements must be encompassed; it is not sufficient to examine just a subset as is done here. The focus on access authorization requirements is for illustrative purposes.

The example shows only the analytical tasks performed in basic evaluation. It does not address planning, initially learning about the application, performing detailed evaluation work, or reporting on findings. Furthermore, it does not address the question of whether access authorization functions are actually being used. Instead, it is concerned only with verifying that the functional capabilities and administrative procedures are in place.

H.2 Requirements Evaluation

The most difficult task in basic evaluation is the critical review (or formulation) of security requirements. This example assumes that, based on analyses of policy and situational needs, the generic access authorization requirements in Figure H-1 are determined to be appropriate for the application in question.

SUBJECTS:	Individuals (not terminals or groups)
OBJECTS:	Data Files (not records or fields)
MODES OF ACCESS:	Read Read and Write Execute Only
DECISION CRITERIA:	Access list showing Subject-Object-Mode of access (not passwords, data values or internal security labels)
CONTROL OF AUTHORIZATION DATA:	Restrictive default policy, i.e., default to denial of access.
SYSTEM RESPONSE:	Denial and continuation of session. Denial and termination of session (no notification of security personnel).
SECURITY LOGGING:	Loggable events — Access denials — Modifications to authorization data Contents of log entries — Unique subject identifier — Date and time — Nature of event — Object

Figure H-1. *Generic functional requirements for access authorization*

H.3 Functional Evaluation

The first step in functional evaluation is determining whether application people and application documentation indicate agreement and compliance with the security requirements. The primary people to consult are managers and users of the application. The remainder of this section summarizes the key documentation to examine.

A primary document to analyze in this step is the Functional Requirements Document. The Functional Requirements Document should include the following information on access authorization:

1. Description of subjects and objects.

2. Statement of access rules.

3. Designation of authorizers.

4. Description of required functional capabilities.

5. Summary of influential security requirements and policy directives.

If this information is provided, the application needs no further functional evaluation for the items listed. If such information is not provided, further analysis is needed.

Other primary documents are those associated with any prior security certifications of the application. These include the security evaluation report and the accreditation statements. The former in particular should contain findings that indicate past compliance with requirements.

The secondary documents to analyze are procedure documents associated with control of the authorization data. Procedures for controlling authorization data usually reveal the nature of subjects, objects, modes of access, decision criteria, and system response, as well as whether there is a restrictive default policy.

The third area of documentation to analyze is the security log. This reveals whether all appropriate loggable events are included and whether the contents of log entries are complete. Next to be examined are procedures relating to review and control of the security log. Effective procedures should:

1. Assign responsibility for reviewing the log.

2. Define the maximum time intervals between reviews and the minimal period for retention of the log.

3. Define what constitutes a security or access violation.

4. Identify actions to take (and avoid) when a violation occurs.

5. Ensure the security of the log.

The product of this step is a listing of functional access authorization capabilities that the application is claimed to possess, along with a list of its applicable administrative procedures.

H.4 Control Existence Determination

Control existence determination testing is required to verify the existence of access authorization functions. The intent is not to assess in detail the quality of the functions—that is beyond the scope of this effort and requires a detailed security evaluation. The intent, rather, is simply to verify that the functions exist. The actual testing required is minimal. In most cases a short operational demonstration suffices. Figure H-2 shows an example.

Several comments are needed to clarify the example.

1. Initialization of the tables might not be an on-line capability. Nevertheless, it is important for the evaluator to monitor the initialization process in person, rather than to simply accept a document showing that it has occurred. Otherwise there is no verification that the restrictive default policy exists.

I. Initialize the Tables

	File B	File C	File D	Trans. X	Prog. Y	Prog. Z
User A	Read	Read/Write		Execute	Execute	

Set system response for Program Z to Denial with Termination.
Set system response for all other objects to Denial with Continuation.

II. Demonstrate Operation

1. Attempt user A access file B — allowed.
2. Attempt user A write file B — not allowed.
3. Attempt user A execute file B — not allowed.
4. Attempt user A access file C — allowed.
5. Attempt user A write file C — allowed.
6. Attempt user A access file D — not allowed.
7. Attempt user A access transaction X — allowed.
8. Attempt user A execute transaction X — allowed.
9. Attempt user A access program Y — allowed.
10. Attempt user A execute program Y — allowed.
11. Attempt user A read program Y — not allowed.
12. Attempt user A write program Y — not allowed.
13. Attempt user A access program Z — not allowed; termination.

Figure H-2. *Illustrative demonstration of access authorization capabilities*

2. Log entries are checked throughout the demonstration to ensure that loggable events are recorded and that the contents of log entries are complete.

3. Where actions are "not allowed" by the access authorization mechanism, checks are needed to verify that the actions have not actually taken place. For example, where a write is not allowed, there is a check that the write attempt has not changed the object.

4. While it is not the purpose of control existence determination to assess the quality of functions, quality must be kept in mind in the event there are gross or fundamental shortcomings that call into question the overall effectiveness of the functions. The most vulnerable area here is authorization table initialization, where inadequate security controls or high susceptibility to human errors could render the mechanism ineffective.

5. The example shows denial with termination and continuation to be keyed around objects. The requirements state only that the capabilities exist. In some cases the capabilities might be keyed around subjects, modes of access, or even the application as a whole.

6. The decision criterion stated in the requirements (i.e., a subject-object-mode of access check) is shown implicitly. The only way to show this explicitly is to examine the program code. Other potential decision criteria (e.g., data values, date and time of day) could be explicitly demonstrated by tests, but these other criteria are not required.

The product of this step is an assessment of whether the functional capabilities listed in the preceding functional evaluation step actually exist.

H.5 Methodology Review

The final step is to briefly examine the methodology used to develop and maintain the access authorization mechanism. As with control existence determination above, the intent is to ensure that there are no fundamental shortcomings that call into question the overall effectiveness of the access authorization mechanism. Following are the primary areas of concern. This methodology review step is mainly concerned with in-house development, but several of the areas of concern can also apply to vendor-provided mechanisms.

1. Is documentation current, complete, and of acceptable quality?

2. Is development well controlled? Are independent reviews and testing performed? Is an effective change control program used?

3. Are effective design and programming practices and standards used?

The product of this step is an assessment of whether the development and maintenance methodology can be relied upon to acceptably reduce the likelihood of major errors.

H.6 Conclusion

Several points are brought out by this example:

1. Accurate, complete, and understandable requirements are critical.

2. Given such requirements, insight and experience are still needed on the part of security evaluators.

APPENDIX I

PREPARATION OF THIS GUIDELINE

In order that readers may better assess and understand this Guideline, this appendix summarizes the sequence of events involved in its production. In general, the events consisted of (1) the performance of a technology assessment on methods to measure the level of computer security, (2) a search for and investigation of existing certification and accreditation programs in Federal agencies, and (3) several invitational mini-workshops to define and discuss issues pertaining to the Guideline itself.

The technology assessment [NBS83] was performed to determine the state of the art in techniques applicable to computer security evaluation. The primary component of the assessment was an investigation of existing security evaluation, risk assessment, and Electronic Data Processing (EDP) audit methodologies. Strengths, weaknesses, and areas of applicability of each were examined. The work included analysis of types of acceptance criteria and examination of the influences of environment and sensitivity distinctions on the evaluation process. Analysis was also performed on the nature and roles of alternative control categorizations. Preparation of the technology assessment involved a substantial literature survey and interaction with many government and industry experts in the fields of computer security, risk assessment, and EDP auditing.

On completion of the technology assessment, a search was conducted for existing Federal government computer security certification programs. More than 40 agencies were contacted for information about existing or planned programs. Based on this effort, four agencies were selected and interviewed in more depth on the nature of and analysis behind their methodologies. These were the Department of Agriculture, the Department of Housing and Urban Development, the Federal Aviation Administration, and the Public Health Service.

On April 2, 1981, an invitational mini-workshop was held at NBS to discuss major computer security certification and accreditation issues. The basic purpose of the workshop was to draw upon existing government certification and accreditation experience to help define the boundaries and general contents of this Guideline. Attendees were divided into two working groups as listed below.

Group A

Zella G. Ruthberg, National Bureau of Standards, Leader
Benjamin Brown, Nuclear Regulatory Commission
Morey Chick, General Accounting Office
Duane Fagg, Naval Data Automation Command
John Gilligan, System Development Corporation
Gregory Loss, Public Health Service
Charles Neam, Federal Aviation Administration
Anna Patrick, Department of Agriculture
Russell Rice, National Aeronautics and Space Administration
Mervyn Stuckey, Department of Housing and Urban Development
Stephen Walker, Office of the Assistant Secretary of Defense

Group B

William Neugent, System Development Corporation, Leader
Stephen Barnett, National Security Agency
Donald Colner, National Bureau of Standards
Edward Joslin, Department of Agriculture
Stuart Katzke, National Bureau of Standards
Terry Losonsky, Department of Defense Computer Institute
Harold Podell, General Accounting Office
William Riggle, Federal Aviation Administration
Peter Tasker, MITRE Corporation
Fred Weingarten, Information Policy Inc.

Based on the findings from the mini-workshop, an initial draft of the Guideline was prepared.

The draft was reviewed at a second NBS mini-workshop on December 14, 1981, with the following attendees:

Zella G. Ruthberg, National Bureau of Standards, Workshop Leader
Stephen Barnett, National Security Agency
Benjamin Brown, Nuclear Regulatory Commission
Edward Joslin, Department of Agriculture
Terry Losonsky, Naval Data Automation Command
Gregory Loss, Public Health Service
Charles Neam, Federal Aviation Administration
William Neugent, System Development Corporation
Anna Patrick, Department of Agriculture
Harold Podell, General Accounting Office
Russell Rice, National Aeronautics and Space Administration
William Riggle, Federal Aviation Administration
Dennis Ruth, Department of Defense Computer Institute
Hilda Sigda, Department of the Interior
Mervyn Stuckey, Department of Housing and Urban Development
John Vasak, System Development Corporation

Based on comments from this mini-workshop, a second draft was prepared and circulated for review to both prior reviewers and to Senior ADP Management Officials at all Federal agencies. On July 12, 1982, an invitational seminar was held at NBS to present the Guideline and solicit final comments. Attendees included both former participants and many Federal managers responsible for information system policy. The final version of the Guideline was then prepared.

In addition to those people above, many others have also critically reviewed the document and submitted comments that influenced the final version. These people include the following:

Sheila Brand, Bruce J. Campbell, D. Glen Dale, Daniel Edwards, Alvin Foster, Lea Hamilton, Frederic A. Heim, Jr., Robert V. Jacobson, Stanley Jarocki, John A. Keenan, Phillip B. Ladd, William LaPlant, Louis N. Lushina, Rhoda R. Mancher, Stan Mashakas, Daniel Mechelke, Fred McBride, Phillip Morrison, Grace H. Nibaldi, Lawrence Noble, William E. Perry, K. A. Rogowski, Robert S. Roussey, Roger R. Schell, James B. Thomas, Jr., Bruce F. Wellborn, and Richard H. Wilcox.

The principal author of the Guideline was William Neugent. Technical direction, oversight, and editing were provided by Mrs. Zella G. Ruthberg. The NBS technical representative was Dr. Stuart Katzke.

APPENDIX J

REFERENCES[1]

[AAC78] A Guide for Studying and Evaluating Internal Accounting Controls, Arthur Andersen & Co., January 1978. (1.5.4, 2.4.2.2)

[AFI79] Security: Checklist for Computer Center Self-Audits, AFIPS Press, 1979. (1.5.3, 2.3.1, 3.3.2.1)

[AKE80] Akers, Sheldon, "Test Generation Techniques," *Computer*, Vol. 13, No. 3, March 1980. (2.4.1.3)

[CIC75] Rosen, R. J., R. J. Anderson, L. H. Chant, J. B. Dunlop, J. C. Gambles, D. W. Rogers, "Computer Audit Guidelines," The Canadian Institute of Chartered Accountants, 1975. (1.5.4, 2.3.1, 2.3.2)

[DOCRP1] Standard Practice for Fire Protection of Essential Electronic Equipment Operation, Department of Commerce Publication RP-1. (C)

[DOD79] ADP Security Manual—Techniques, and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems, DoD 5200.28-M, 25 June 1979. (1.5.3, B)

[DOD80] DoD Policy Survey Subcommittee, *Survey of Federal Computer Security Policies*, November 1980. (B)

[DOD83] Department of Defense Trusted Computer System Evaluation Criteria, DoD Computer Security Center, CSC-STD-001-83, August 15, 1983. (2.1.2.3, 2.3.1, 2.5.1, B)

[EAF83] Control Objectives-1983, EDP Auditors Foundation for Education and Research, 1983. (2.3.1, 3.3.2.1)

[EPP80] Epperly, Eugene V., "The Department of Defense Computer Security Initiative Program and Current and Future Computer Security Policies," *Proceedings of the Second Seminar on the DoD Computer Security Initiative Program,* January 15-17, 1980. (C)

[FAA80] Security Certification Guidelines for the Federal Aviation Administration's Uniform Payroll System, prepared by EDP Audit Controls, Inc., for the FAA, October 1980. (2.7.2, B)

[FAIM] EDP Security, Security Review of EDP Data, Facilities, and Personnel, Faim Technical Library, no date. (2.3.1)

[FIPS11] Dictionary for Information Processing, FIPS PUB 11-1, September 1977. (1.2.5, A)

[FIPS31] Guidelines for Automatic Data Processing Physical Security and Risk Management, FIPS PUB 31, June 1974. (2.2.1, 2.3.1, A, B)

[FIPS38] Guidelines for Documentation of Computer Programs and Automated Data Systems, FIPS PUB 38, February 1976. (2.3.1, 2.3.2, A, B, F)

[FIPS39] Glossary for Computer Systems Security, FIPS PUB 39, February 1976. (1.2.3, 1.2.4, A, B)

[FIPS41] Computer Security Guidelines for Implementing the Privacy Act of 1974, May 1975. (B)

[FIPS64] Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase, FIPS PUB 64, August 1979. (2.3.2, B, F)

[FIPS65] Guideline for Automatic Data Processing Risk Analysis, FIPS PUB 65, August 1979. (1.5.1, 2.2.1, 2.3.1, 2.4.2.1, A, B)

[FIPS73] Guidelines for Security of Computer Applications, FIPS PUB 73, June 1980. (1.2.7, 2.3.1, 2.3.2, 2.3.4, B, F)

[FIPS83] Guideline on User Authentication Techniques for Computer Network Access Control, FIPS PUB 83, September 1980. (2.4.1.2)

[1]. Parenthetical section numbers indicate where the references are made.

[FIPS87] Guidelines for ADP Contingency Planning, FIPS PUB 87, March 1981 (1.4, 2.3.2, 2.4.1.2, 2.4.2, B)

[FIPS88] Guideline on Integrity Assurance and Control in Database Administration, FIPS PUB 88, August 1981. (A, B)

[FIPS101] Guideline for Lifecycle Validation, Verification, and Testing of Computer Software, to be published in 1983. (1.5.2, 2.3.4, 2.4.1.1, F)

[FIT78] FitzGerald, Jerry, "Internal Controls for Computerized Systems," Jerry FitzGerald & Associates, 1978. (1.5.3, 2.3.1, 3.3.2.1)

[FIT81] FitzGerald, Jerry, "Designing Controls into Computerized Systems," Jerry FitzGerald & Associates, 1981. (2.3.1, 3.2.2)

[GAO81-1] Government-Wide Guidelines and Management Assistance Center Needed to Improve ADP Systems Development, U.S. General Accounting Office, AFMD-81-20, February 26, 1981. (B, F)

[GAO81-2] Evaluating Internal Controls In Computer-Based Systems—Audit Guide, U.S. General Accounting Office, AFMD-81-76, June 1981. (1.5.4, 2.3.1, 2.3.2, 2.4.1.1, 3.3.2.1, B)

[GAO81-3] Assessing Reliability of Computer Output—Audit Guide, U.S. General Accounting Office, AFMD-81-91, June 1981. (1.5.4, 1.5.5)

[GAO82-1] Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices, U.S. General Accounting Office, MASAD-82-18, April 21, 1982. (1.4, B, C)

[GAO82-2] U.S. General Accounting Office, Denver Regional Office Report, "Improving Generalist's Capabilities in Assessing Output Reliability and Internal Controls in Computer-Based Systems," October 1982. (2.1)

[HHS78] Part 6, ADP Systems Security, Department of Health and Human Services (HHS) ADP Systems Manual, 14 September 1978. (2.3.1, B)

[HOF80] Hoffman, L. J. and Neitzel, L. A., "Inexact Analysis of Risk," *Proceedings of the 1980 IEEE International Conference on Cybernetics and Society,* October 1980. (1.5.1)

[HOL74] Hollingworth, D., S. Glaseman, M. Hopwood, "Security Test and Evaluation Tools: An Approach to Operating System Security Analysis," P-5298, The Rand Corporation, September 1974. (2.4.1.3)

[IBM76] Attanasio, C. R, P. W. Markstein, R. J. Phillips, "Penetrating an Operating System: A Study of VM/370 Integrity," *IBM Systems Journal,* No. 1, 1976. (2.4.1.3)

[IBM80] Security Assessment Questionnaire, IBM Data Processing Division, GX20-2381-0, 1980. (2.1, 2.3.1, 2.3.2)

[IIA77-1] Ruder, Brian, Tom S. Eason, Malin E. See, Susan Higley Russell, "Systems Auditability and Control; Data Processing Audit Practices Report," prepared by Stanford Research Institute for The Institute of Internal Auditors, Inc., under a grant from IBM Corp., 1977. (2.4.1.1, 2.4.2.2)

[IIA77-2] Russell, Susan Higley, Tom S. Eason, J. M. FitzGerald, "Systems Auditability and Control; Data Processing Control Practices Report," prepared by Stanford Research Institute for The Institute of Internal Auditors, Inc., under a grant from the IBM Corp., 1977. (3.3.2.1)

[IST79] RAMP, What It is. . . ., How To Use It. . . ., What It Does. . . ., International Security Technology, Inc., 1979. (1.5.1)

[KON81] Konigsford, William L., "Developing Standards for Operating System Security," *Computer Security Journal,* Spring 1981. (2.3.1)

[LIN75] Linde, Richard R., "Operating System Penetration," *National Computer Conference Proceedings,* AFIPS Press, 1975. (2.4.1.3, 3.3.2.1)

[MAI76] Mair, William C., Donald R. Wood, Keagle W. Davis, "Computer Control & Audit," The Institute of Internal Auditors, 1976. (1.5.4, 2.1.2.5, 2.2.1, 2.3.2, 2.4.1.1, A)

[NASA82] Giragosian, Paul A., David W. Mastbrook, Frederick G. Tompkins, ''Guidelines for Certification of Existing Sensitive Systems,'' The MITRE Corporation - METREK Division, MTR-82W18, prepared for the National Aeronautics and Space Administration, July 1982. (2.1.2.3)

[NBS77] Ruthberg, Zella G., Robert G. McKenzie (Editors), ''Audit and Evaluation of Computer Security,'' NBS Special Publication 500-19, October 1977. (2.3.1)

[NBS80] Ruthberg, Zella G. (Editor), ''Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls,'' NBS Special Publication 500-57, April 1980. (1.2.5, 2.3.1, A)

[NBS81] Adrion, W. Richards, Martha A. Branstad, John C. Cherniavsky, ''Validation, Verification, and Testing of Computer Software,'' NBS Special Publication 500-75, April 1980. (2.3.1, 2.4.1.1, A)

[NBS82-1] Powell, Patricia B. (Editor), ''Software Validation, Verification, and Testing Technique and Tool Reference Guide,'' NBS Special Publication 500-93, September 1982. (2.4.1.1)

[NBS82-2] Houghton, Raymond C., Jr., ''Software Development Tools,'' NBS Special Publication 500-88, March 1982. (2.3.4, 3.3.3.2)

[NBS82-3] Powell, Patricia B., ''Planning for Software Validation, Verification, and Testing,'' NBS Special Publication 500-98, November 1982. (2.3.4)

[NBS83] Ruthberg, Zella G. (Editor), William Neugent, John Gilligan, and Lance Hoffman, ''Technology Assessment: Methods for Measuring the Level of Computer Security,'' NBS Special Publication __, (currently in draft—September 1981). (1.5, 2, 2.1.2.4, 2.3.1, 2.3.2, 2.3.4, 2.3.5, 2.4.1.1, 2.4.2.1, 2.4.2.2, I)

[NEU78] Neumann, Peter G., ''Computer System Security Evaluation,'' *National Computer Conference Proceedings*, AFIPS Press, 1978. (2.4.1.3, 3.3.2.1)

[NEUG82] Neugent, William, ''Acceptance Criteria for Computer Security,'' *National Computer Conference Proceedings,* AFIPS Press, 1982. (1.5.1, 2.3.1, 2.4)

[NIE80] Nielsen, Norman R., Brian Ruder, ''Computer System Integrity Vulnerability,'' *Information Privacy,* Vol. 2, No. 1, January 1980. (2.4.2.1)

[OMB78] Security of Federal Automated Information Systems, Office of Management and Budget (OMB) Circular No. A-71 (Transmittal Memorandum No. 1), effective July 27, 1978. (1.2.7, 1.5.1, 2.3.2, 2.5.3, 2.7.1, A, B)

[OMB81] Internal Control Systems, OMB Circular No. A-123, 28 October 1981. (2.1.2.3, 2.3.1, 2.7.1, A, B)

[PMM80] Data Processing Security Evaluation Guide (DPSE), 1980, Peat, Marwick, Mitchell & Co. (1.5.3, 1.5.4, 2.1.2.4)

[PRA80] Paperwork Reduction Act of 1980. (A, B)

[SDC79] Risk Assessment Methodology, System Development Corporation, TM-WD-7999/001/03, prepared for the Naval Data Automation Command, July 1979. (1.5.1, 2.3.1, A)

[SIP72] Sippl, Charles J., Charles P. Sippl, *Computer Dictionary and Handbook,* 1972. (1.2.5, 1.2.6, A)

[USA380] Automated Systems Security, U.S. Army Regulation 380-380. (C)

[USAF82] Interim Policy Guidance for Security of Air Force Automated Data Processing (ADP) Systems, Headquarters USAF (ACD), 13 July 1981. (A,F)

[WEB76] Webster's New World Dictionary of the American Language, Second College Edition, William Collins & World Publishing Co., Inc., 1976. (A)

[WEBB76] Webb, Doug A., W. G. Frinkel, et al., ''Handbook for Analyzing the Security of Operating Systems,'' Lawrence Livermore Laboratory (LLL), 1 November 1976. (1.2.5, 2.4.1.3)

[WEI73] Weissman, Clark, ''System Security Analysis/Certification Methodology and Results,'' System Development Corporation SP-3728, 8 October 1973. (2.4.1.3)

☆U.S.GOVERNMENT PRINTING OFFICE:1989-242-200/00041

NBS TECHNICAL PUBLICATIONS

PERIODICALS

JOURNAL OF RESEARCH—The Journal of Research of the National Bureau of Standards reports NBS research and development in those disciplines of the physical and engineering sciences in which the Bureau is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Bureau's technical and scientific programs. As a special service to subscribers each issue contains complete citations to all recent Bureau publications in both NBS and non-NBS media. Issued six times a year. Annual subscription: domestic $18; foreign $22.50. Single copy, $5.50 domestic; $6.90 foreign.

NONPERIODICALS

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NBS, NBS annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NBS under the authority of the National Standard Data Act (Public Law 90-396).

NOTE: The principal publication outlet for the foregoing data is the Journal of Physical and Chemical Reference Data (JPCRD) published quarterly for NBS by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements available from ACS, 1155 Sixteenth St., NW, Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NBS administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order the above NBS publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.

Order the following NBS publications—FIPS and NBSIR's—from the National Technical Information Service, Springfield, VA 22161.

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NBS 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 CFR (Code of Federal Regulations).

NBS Interagency Reports (NBSIR)—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.