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 secuity. [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.