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; approve 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.

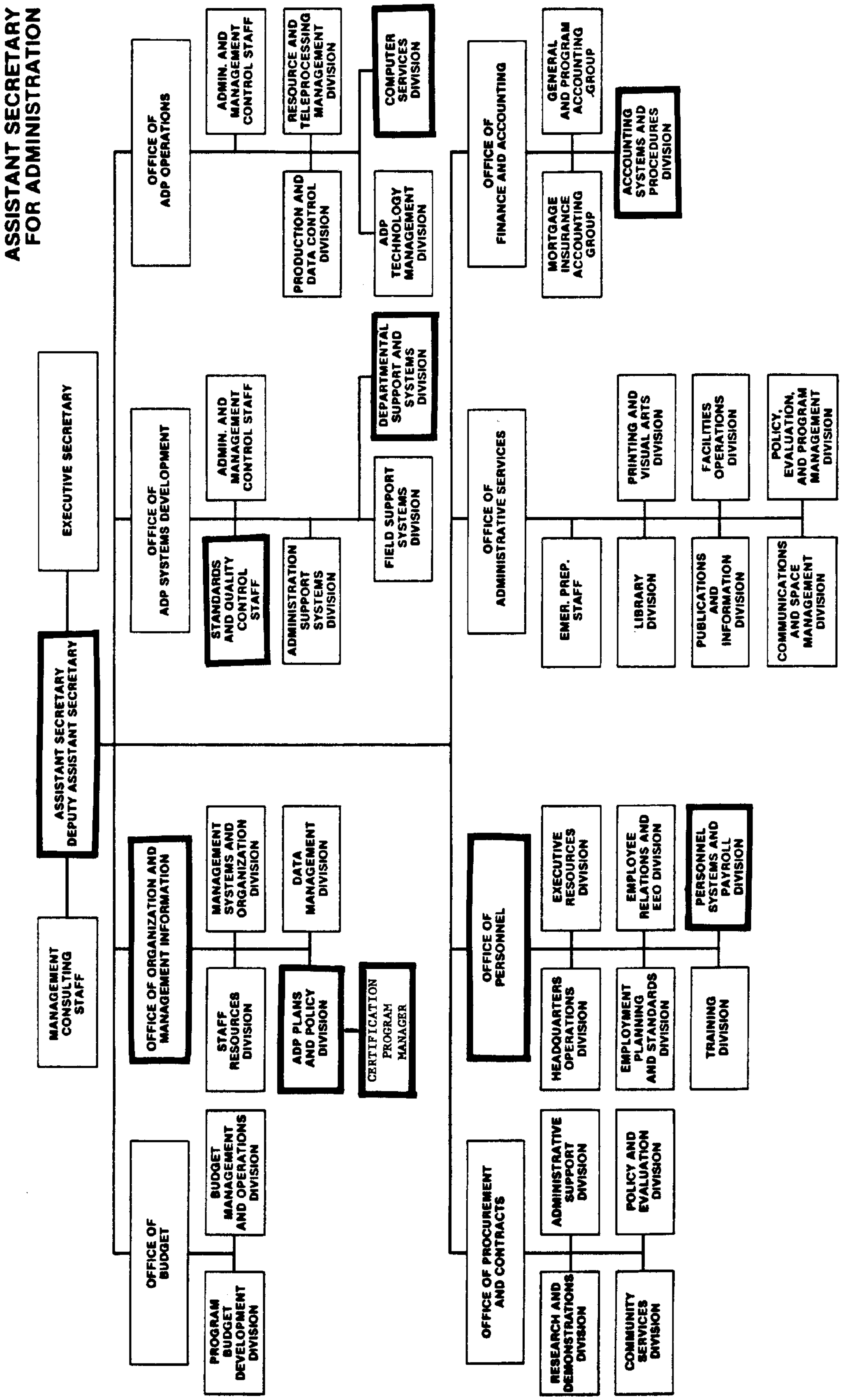
ASSISTANT SECRETARY FOR ADMINISTRATION
MANAGEMENT CONSULTING STAFF
ASSISTANT SECRETARY DEPUTY ASSISTANT SECRETARY
EXECUTIVE SECRETARY
OFFICE OF BUDGET
PROGRAM BUDGET DEVELOPMENT DIVISION
BUDGET MANAGEMENT AND OPERATIONS DIVISION
OFFICE OF ORGANIZATION AND MANAGEMENT INFORMATION
STAFF RESOURCES DIVISION
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