

GAO

Report to the Chairman, Committee on
Science, Space, and Technology, House of
Representatives

May 1988

INFORMATION
SYSTEMS

Agencies Overlook
Security Controls
During Development



released
RESTRICTED—Not to be released outside the General
Accounting Office except on the basis of the specific approval
by the Office of Congressional Relations.

042317

4 *

Foreword

On May 31, 1988, the U.S. General Accounting Office (GAO) issued to the Chairman, House Committee on Science, Space, and Technology, a report entitled *Information Systems: Agencies Overlook Security Controls During Development* (GAO/IMTEC-88-11). The report showed that the nine agencies reviewed were not meeting federal criteria and good system development practices—as described in the GAO model—for providing reasonable assurance that appropriate security controls were being successfully incorporated into the development of their automated information systems. This supplement presents the details of the model that served as the criteria underlying our assessments. Also presented are potential effects of not successfully incorporating appropriate security controls into system development. For further information contact Dr. Harold J. Podell, Group Director, at 275-9595.

Contents

Foreword		1
Appendix I		4
Model of Security in the System Life Cycle Development Process		4
	Section A: Discussion of Standards and Use	4
	Section B: Sub-Activities of GAO Audit Model of Security Development	16
	Initiation Phase	16
	Definition Phase	23
	Design Phase	36
	Construction Phase	41
	Integration, Installation, and Test Phase	43
	Section C: Potential Effects of Not Performing Security Activities During System Development	62
Glossary		70
Bibliography		80
Figures		
	Figure I.1: Model of Security in the System Life Cycle Development Process: Initiation Phase	8
	Figure I.2: Model of Security in the System Life Cycle Development Process: Definition Phase	10
	Figure I.3: Model of Security in the System Life Cycle Development Process: Design Phase	12
	Figure I.4: Model of Security in the System Life Cycle Development Process: Construction Phase	13
	Figure I.5: Model of Security in the System Life Cycle Development Process: Integration, Installation, and Test Phase	14
	Figure I.6: Potential Effects of Not Performing Security Activities During System Development: Initiation Phase	62
	Figure I.7: Potential Effects of Not Performing Security Activities During System Development: Definition Phase	64
	Figure I.8: Potential Effects of Not Performing Security Activities During System Development: Design Phase	66

Figure I.9: Potential Effects of Not Performing Security Activities During System Development: Construction Phase	67
Figure I.10: Potential Effects of Not Performing Security Activities During System Development: Integration, Installation, and Test Phase	68

Abbreviations

ADP	automated data processing
ADPE	automated data processing equipment
APR	agency procurement request
DOD	Department of Defense
DODCI	Department of Defense Computer Institute
DODCSC	Department of Defense Computer Security Center
EPL	evaluated products list
FIPS	Federal Information Processing Standards
FIRMR	Federal Information Resources Management Regulation
FPM	Federal Personnel Manual
GAO	General Accounting Office
GAO Yellow Book	Standards for Audit of Governmental Organizations, Programs, Activities, and Functions
IMTEC	Information Management and Technology Division
ISO	International Organization for Standardization
LCM	life cycle management
MIL STD	military standard
NBS	National Bureau of Standards
NCSC	National Computer Security Center
NSDD	National Security Decision Directive
OMB	Office of Management and Budget
PCIE	President's Council on Integrity and Efficiency
PCMI	President's Council on Management Improvement
PCMI/PCIE	President's Council on Management Improvement/President's Council on Integrity and Efficiency 1986, 1987 publications on a model framework for management control over automated systems
TCSEC	Trusted Computer System Evaluation Criteria

Model of Security in the System Life Cycle Development Process

Section A: Discussion of Standards and Use

This appendix is divided into three sections. Section A entitled, Model of Security in the System Life Cycle Development Process: Discussion of Standards and Use, explains how the model is constructed. Section B entitled, Sub-activities of GAO Audit Model of Security Development, provides the detailed sub-activities of the model. Section C entitled, Potential Effects of Not Performing Security Activities During System Development, presents the potential effects of not performing security activities during system development. This section demonstrates to management the importance of incorporating security for systems in development.

Description of Security Development Audit Model Standards

The general model of information system development, on which the audit model for security development is based, breaks down the activities associated with the development of an information system into five phases: initiation; definition; design; construction; and integration, installation and test. Our description of the phases focuses on the successive levels of detail achieved as the system moves from an overall concept of functional requirements to an operational collection of hardware, software and network components, and procedures. The general model and our model reflect a "building block" view of this progression in which development steps are dependent upon the decisions and results of earlier steps.

Although the building block development of our security/audit model suggests that the phases must be executed in strict sequence, the model can also represent variations of this strict sequence which cycle back to an earlier step to refine or modify previous decisions and then carry the consequences of these changes forward. "Prototyping," in which cycles repeatedly go through earlier phases of development activity, represents one extreme variation of systems/security development.

The selection of security controls should be based on a thorough understanding of potential security threats to the system, its vulnerabilities, the risks, and various feasible security alternatives. The selection of security controls can be done at one point during a "classical" development cycle or, gradually arrived at through several iterations of prototyping. Similarly, independent of the development methodology employed, this selection decision must precede the final decision on overall systems design and be considered as input to the design.

Our standard of evaluation requires that agency procedures for information systems development provide reasonable, positive, and auditable

assurance that appropriate security controls have been carefully evaluated and successfully incorporated in system development. The burden of proof is placed on the system developers to demonstrate, as a routinely expected by-product of the procedures employed, that this assurance is provided.

Generally accepted practices of software engineering (for example, FIPS 38) call for the complete documentation of a system's requirements, including analysis of alternatives, design, specifications, and tests. Our previous work¹ and the work of others² point to numerous cases of significant defects in security that have not been caught until after system development has been completed and the system put into use. Our 1985 review of the security of 25 selected systems (see footnote 1) suggested the general prevalence of this problem and supported the observation that, lacking positive assurance that adequate security controls had been incorporated into the system, there was risk that the system would be seriously flawed.

Description of the Security Development Model

Our information security model was developed to assist in the assessment of information security for systems in development. We used a framework of life cycle management (LCM)³ to construct the model. Within this framework, we identified the necessary security activities, as mentioned in GAO report, Information System Development: Agencies Give Insufficient Attention to Security Controls (GAO/IMTEC-88-11). In assessing agency practices against our criteria, we reached an overall judgment as to whether

- each of the major decisions affecting the definition of requirements, specification, design, construction, and testing of the overall system included appropriate consideration of security-related factors, and
- these security factors had been arrived at using adequate information on the security needs of the system and the range of security alternatives available, as well as any relevant technical and funding limitations.

¹Testimony of William S. Franklin, Associate Director, before the Subcommittee on Transportation, Aviation and Materials, House Committee on Science and Technology, Oct. 29, 1985.

²U.S. Congress, Office of Technology Assessment, Federal Government Information Technology: Management, Security, and Congressional Oversight, OTA-Cit-297. (Washington, D.C.: U.S. Government Printing Office, Feb. 1986).

³Life cycle management refers to the formal process of directing a system development using a phased-model approach. Our model is an approach to life cycle management.

The model is entitled "Model of Security in the System Life Cycle Development Process" (see figure I.1). In the model the relationship between the life cycle management activities for the system, and the security development processes are shown. The relationship is primarily developed from a software engineering perspective. The model depicts the LCM development, that is, the identification of major activities necessary to develop a system and documents produced at the completion of each activity. These development activities and documents appear on the left side of the model and are sequentially arranged into major phases of development. The major phases of development are: initiation; definition; design; construction; and integration, installation, and test. At the end of each phase, with the exception of the initiation phase, different baselines are presented. These baselines represent the sum total of system and security information developed during all preceding steps. System decision papers appear at the end of each phase and contain information on the decisions made as a result of completing all preceding steps.

We determined the degree of assurance that information security was being incorporated into the system development by comparing the agency practices with the security activities in the right side of the model. There are 21 major security activities and associated documents included in the model. The following notation was used for the model: When a system-level document might contain security information, there is an arrow pointing from the system-level document to the security-level document. These shared information sources are indicated by a dotted line around the document at the security level, whereas "stand alone" security documents are indicated by a solid line.

Although the major security activities on the right side of the model are arranged sequentially, some activities could be and are undertaken concurrently or iteratively. For example, step 4, establishing quality assurance for security controls development, could be undertaken at the same time as step 5, defining security requirements. Additionally, prototyping tools, such as fourth generation software tools, could be used in an iterative manner to assist in certain steps, such as step 5, defining security requirements. When prototyping is used, the automated information system development practices and documentation presented in the model still apply.

The citations to documents, contained in parentheses on the model, are provided as a partial list of sources used. There are specific activities

Appendix I
Model of Security in the System Life Cycle
Development Process

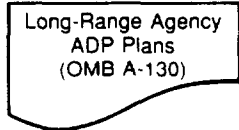
and information that should be documented for each of the major security processes contained in the model. These activities and supporting sub-activities were identified and included on the basis of security expert review and recommendations of security practices to be undertaken during system development. Section B of this appendix contains the specific sub-activities and supporting information related to each of the major security activities.

**Figure I.1: Model of Security in the System Life Cycle Development Process;^a
Initiation Phase**

Operating Environment

System

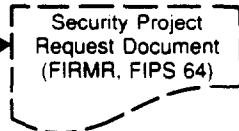
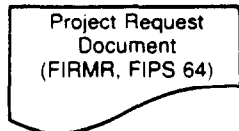
- Long-range strategic ADP plan consistent with agency missions and goals



Security

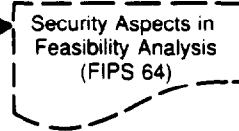
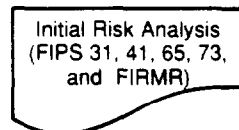
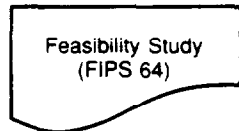
- Management control process to ensure security controls are incorporated into new applications and significant modifications (OMB A-130)
- Agency program in place:
 - Security responsibilities in ADP position descriptions (FIPS 87)
 - Personnel screening (OMB A-130, FPM 732, 736)
 - Security awareness training program (OMB A-130)
 - Configuration management/change control plans (OMB A-130)

- Define and validate need: Identify user needs in context of mission, resources and priority
 - Describe the basic requirements and objectives of the project
 - Provide a general statement concerning the nature of the service requested and the overall concept

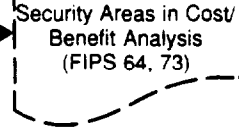
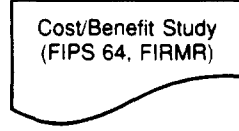


1. Define basic security needs
 - Identify sensitive information and applications (OMB A-130, NSDD 145, FIPS 64, 73)
 - Identify system concepts (preliminary architecture) (FIPS 64)
 - Identify basic security objectives (FIPS 73)
 - Identify privacy and security controls work load (FIRMR)

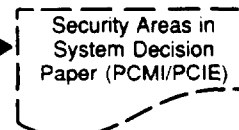
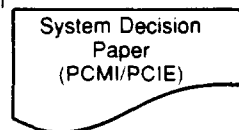
- Evaluate alternatives
 - Identify alternatives to satisfy requirements
 - Analyze technical, operational and economic feasibility
 - Perform comparative cost/benefit analysis



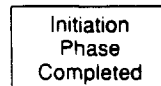
2. Identify security alternatives
 - Identify threats, vulnerabilities, and risks (FIPS 31, 41, 65, 73, FIRMR)
 - Assess technical, operational, and economic feasibility of system security alternatives (FIPS 64, 73)
 - Estimate the security-related cost/benefits of system alternative(s) (FIPS 64, 73)




- Select and approve one alternative plan and approach
 - Establish system objectives and general definition of requirements - overall system architecture



3. Identify basic security framework in the selected system alternative
 - Provide essential information on security issues and risks (PCMI/PCIE)



**Appendix I
Model of Security in the System Life Cycle
Development Process**



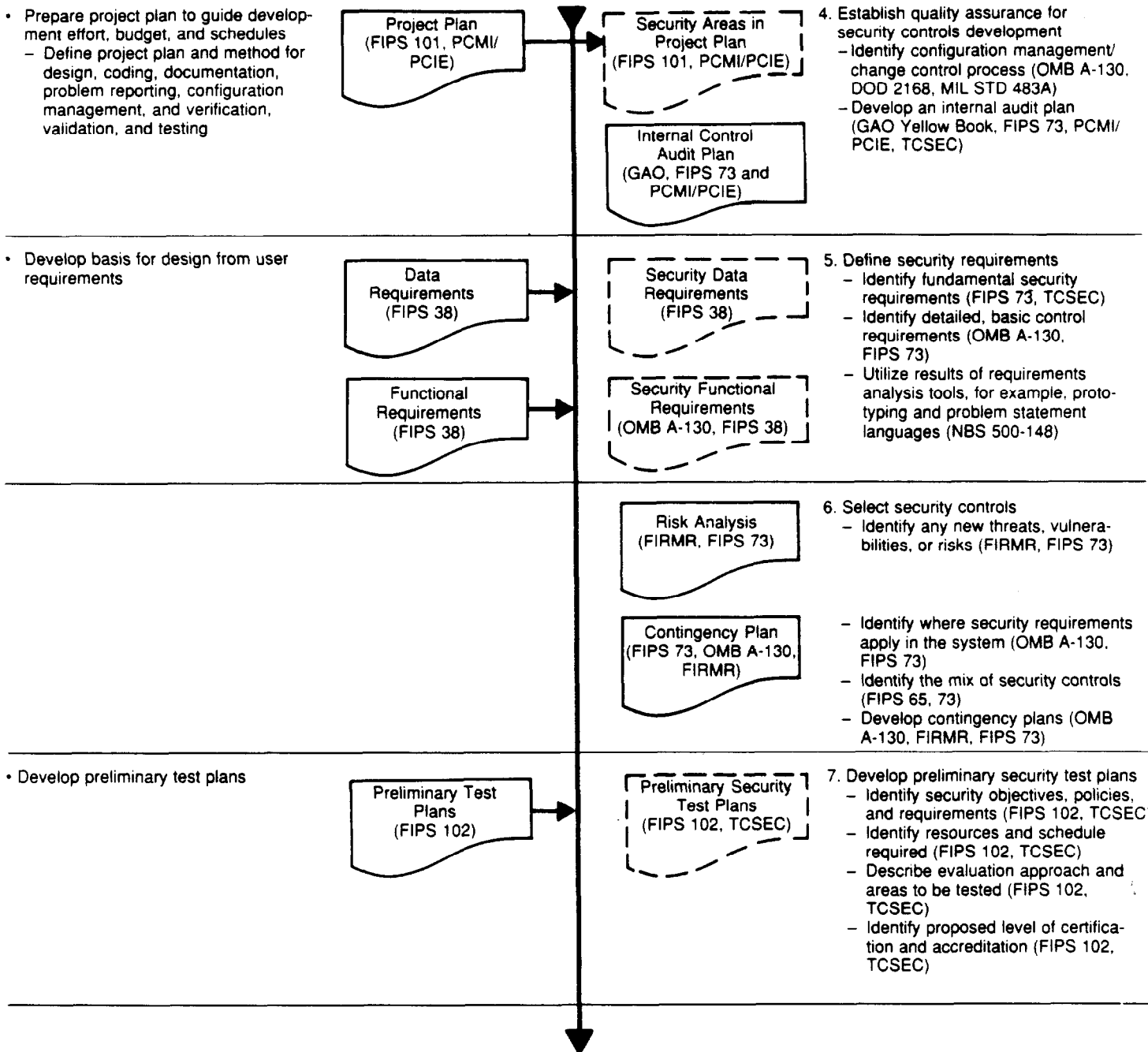
* Not assessed at the nine agencies reviewed.

* Acronyms and abbreviations are spelled out in table of contents.

Note: Shared information sources are indicated by a dotted line around the document at the security level, whereas "stand alone" security documents are indicated by a solid line.

**Appendix I
Model of Security in the System Life Cycle
Development Process**

Figure I.2: Model of Security in the System Life Cycle Development Process*
Definition Phase



**Appendix I
Model of Security in the System Life Cycle
Development Process**

- Select acquisition strategy (for example, major system, field competitive) commensurate with cost, risk, and urgency of need

Solicitation(s) and Contract(s) (FIRMR)

RFP(s), and Contract(s) (FIRMR)

- *8. Design contracts to include security requirements
 - Agency certifies solicitations as meeting security needs (FIRMR)
 - Solicitations provide security controls development quality assurance (FIRMR)
 - Agency evaluates adequacy and presence of security controls in offers (FIRMR)
 - Agency monitors contracts (FIRMR)
 - Procurement request identifies compliance with the Privacy Act of

- Update requirements analysis
- Establish a formal, functional baseline

System Decision Paper (PCMI/PCIE)

Security System Decision Paper (PCMI/PCIE)

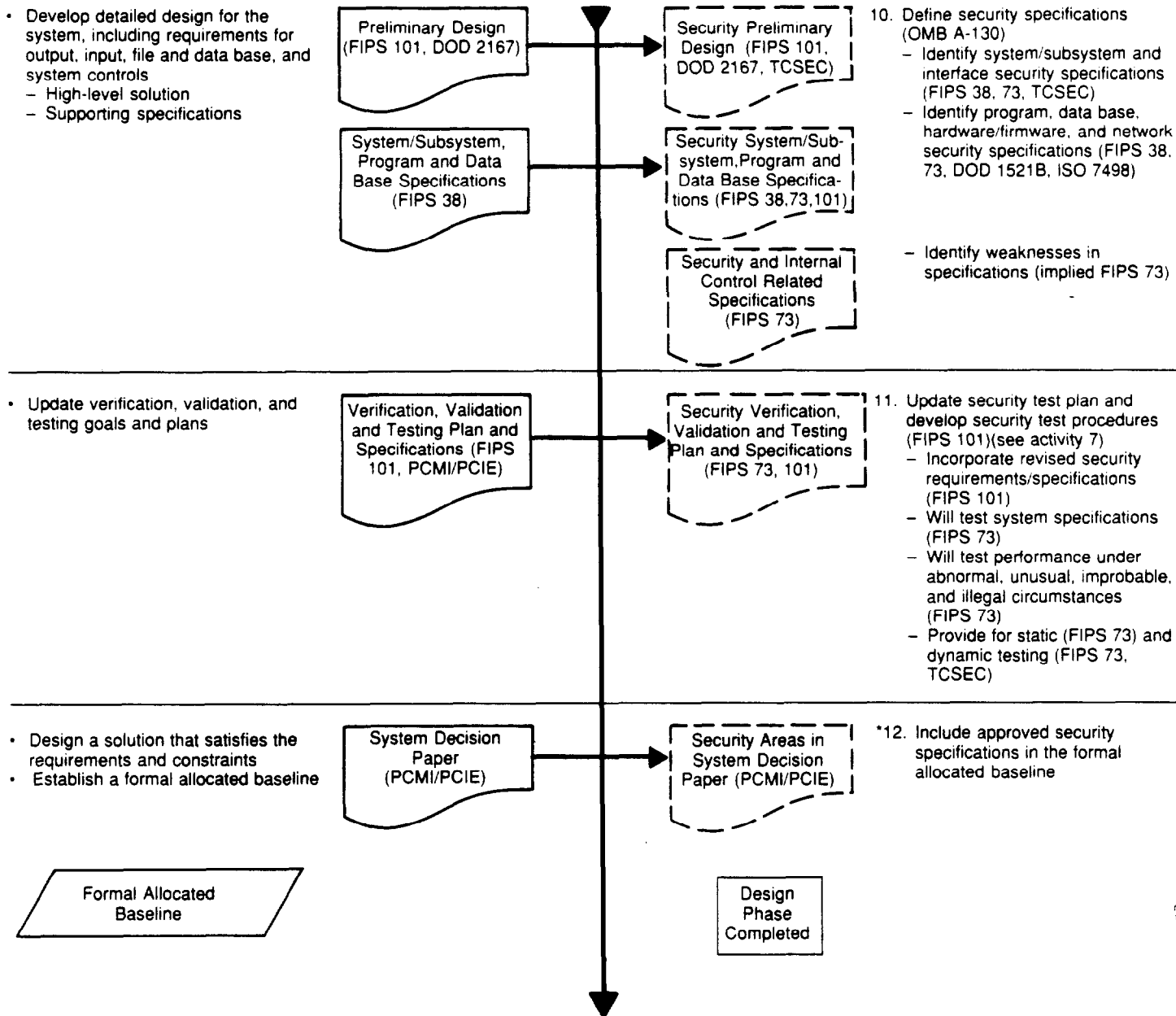
- *9. Include approved security requirements in the formal functional baseline

Formal Functional Baseline (Freeze Requirements)

Definition Phase Completed

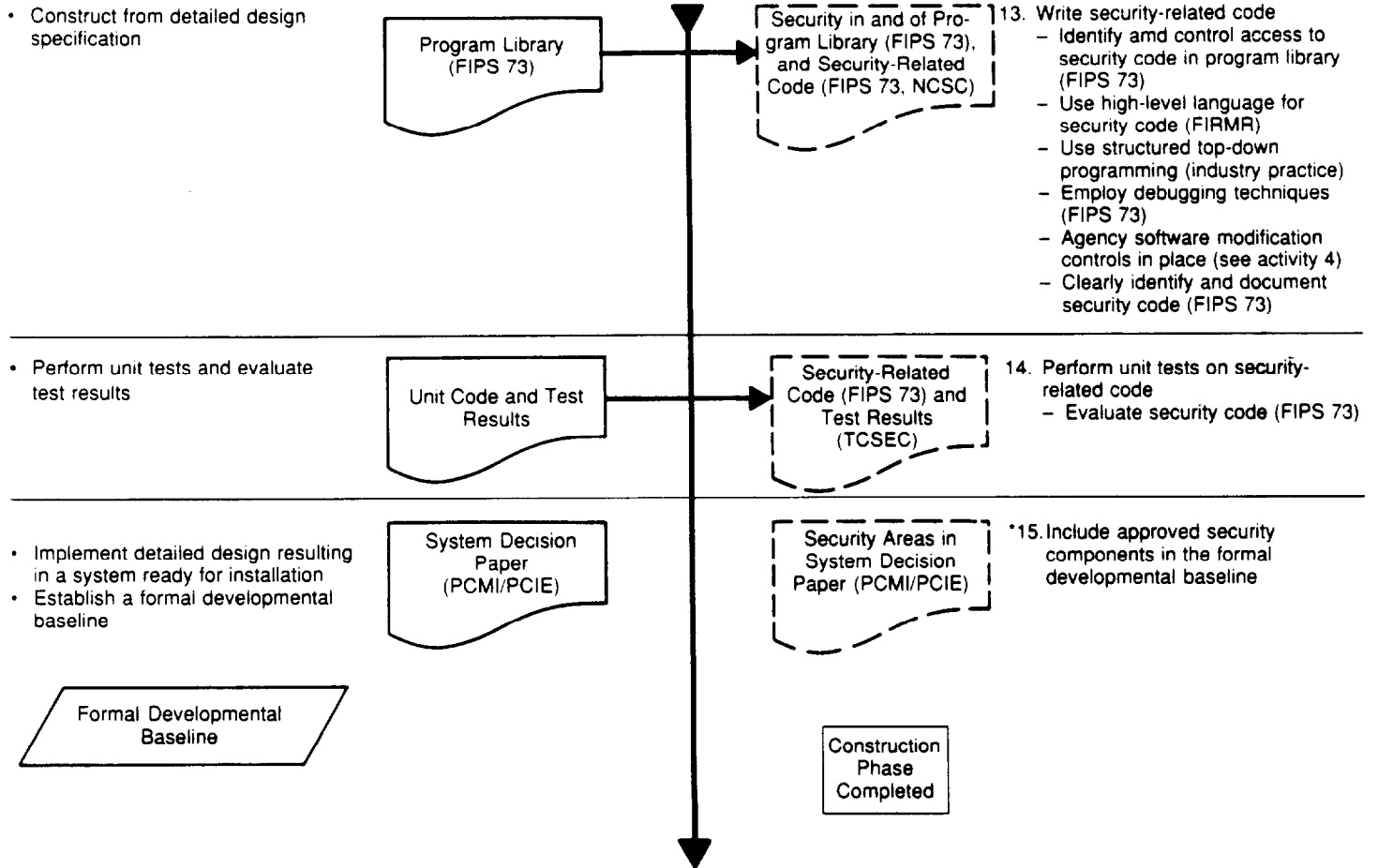
**Appendix I
Model of Security in the System Life Cycle
Development Process**

Figure I.3: Model of Security in the System Life Cycle Development Process*
Design Phase



**Appendix I
Model of Security in the System Life Cycle
Development Process**

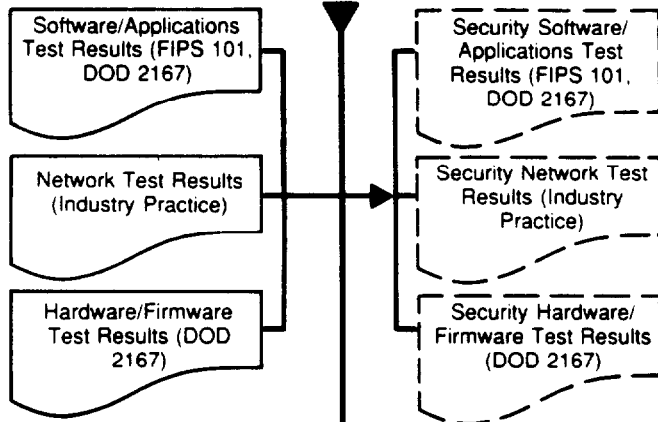
Figure I.4: Model of Security in the System Life Cycle Development Process*
Construction Phase



Appendix I
Model of Security in the System Life Cycle
Development Process

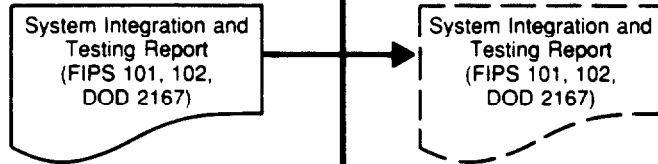
Figure I.5: Model of Security in the System Life Cycle Development Process*
Integration, Installation and Test Phase

• Test system components



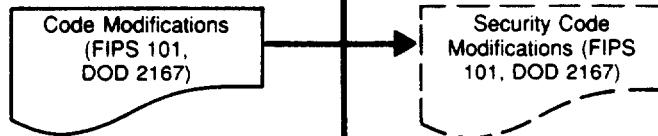
16. Conduct tests of security in the configured components
- Assess software/applications (FIPS 101, 102, DOD 2167)
 - Assess network (ISO 7498)
 - Assess hardware/firmware (DOD 2167)

• Validate system performance through benchmarking and other techniques



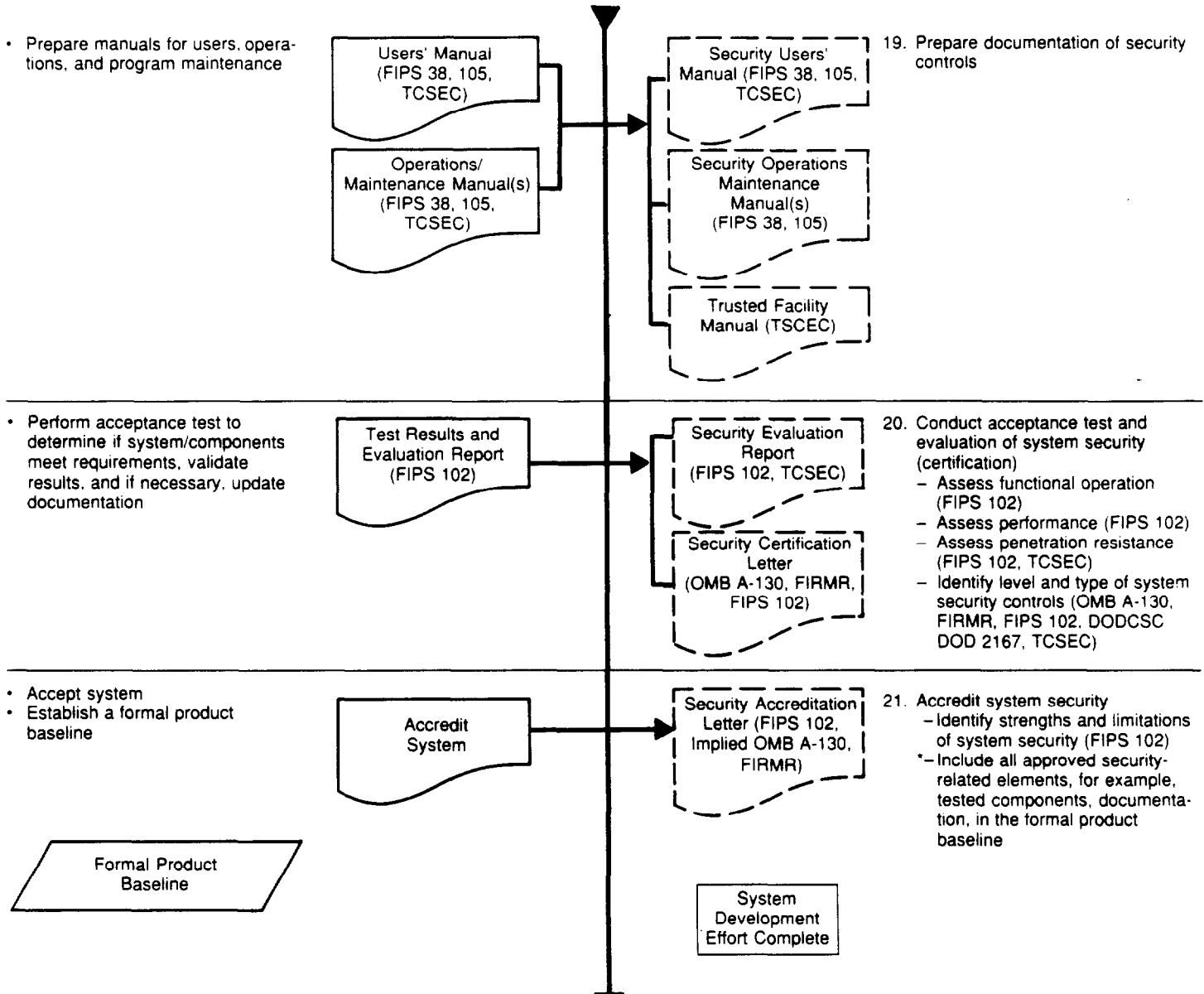
17. Conduct tests of security in the integrated system
- Assess functional operation (FIPS 102)
 - Assess performance (FIPS 102)
 - Identify any test failures (DOD 2167)
 - Tests follow test plans and procedures (implied FIPS 101, 102)
 - Test results are analyzed against security requirements/specifications (DOD 2167)

• Install system



18. Install security code and modify as appropriate (FIPS 101, DOD 2167)

**Appendix I
Model of Security in the System Life Cycle
Development Process**



Section B: Sub-Activities of GAO Audit Model of Security Development

This section of the appendix contains the specific sub-activities and supporting information we believe to be pertinent to the success of the major security activities.

Initiation Phase

1. Define basic security needs.

Sub-activity

Identification of sensitive information or applications to be used in the system.

Information

A. Records about and applications involving individuals requiring protection under the Privacy Act (OMB A-130, p. III-1, FIPS 64, p. 19).

B. Information not releasable under or applications involving the Freedom of Information Act (OMB A-130, p. III-1, FIPS 64, p. 19).

C. Information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission (OMB A-130, p. III-1).

D. Proprietary information (OMB A-130, p. III-1).

E. National security data/applications (National Security Decision Directive 145; FIPS 73, p. 10).

F. Information/applications involving funds disbursement and accounting such as payroll, benefits payments, accounts payable, accounts receivable, and inventory control (FIPS 73, p. 9).

G. Human safety information/applications (FIPS 73, p. 9).

Sub-activity

Description of overall system concepts/preliminary architecture.

Information

A. Service description, such as what functions have to be accomplished within the time period available, information on inputs, processing capabilities, and desired outputs (FIPS 64, p. 19).

B. Relationships to other systems/functions/procedures in terms of common inputs, processing capabilities, and outputs (FIPS 64, p. 19).

C. Organizations affected by the system (FIPS 64, p. 19) including types and locations of users (industry practice).

D. Basic network description, such as the approximate number and location of remote terminals/central processing units (industry practice).

Sub-activity

Identification of basic security objectives in three major areas.

Information

A. Data Integrity—the state that exists when computerized data is the same as that in the source documents, or has been correctly computed from source data and has not been exposed to accidental or malicious alteration or destruction. Erroneous source data and fictitious additions to the data are considered violations of data integrity (FIPS 73, p. 8).

B. Data Confidentiality—the state that exists when data is held in confidence and is protected from unauthorized disclosure. Misuse of data by those authorized to use it for limited purposes is also a violation of data confidentiality (FIPS 73, p. 8).

C. ADP Availability—the state that exists when required ADP services can be obtained within an acceptable period of time (FIPS 73, p. 8).

Sub-activity

Identify the present and future work load in terms of privacy and security controls (FIRMR, Section 201-30.007).¹

2. Identify security alternatives.

This section applies to both new and proposed significant changes to existing systems. If the changes are proposed, previous documentation should be updated as appropriate using the information presented below.

¹ Means that this security-related activity was not assessed at the nine agencies reviewed.

Sub-activity

Threats, vulnerabilities, and risks to the system are identified (FIRMR, Section 201-7.103-2). FIPS 41 provides guidance on Privacy Act considerations and therefore applies to agencies proposing to automate their systems or whose systems contain privacy-related data (FIRMR, Section 201-7.103-4). When systems will not contain privacy data, FIPS 41 information (when the sole citation) should be marked N/A.

Information

A. Threats including:

1. Natural disasters in terms of:

- (a) fire,
- (b) flood,
- (c) earthquake, and
- (d) windstorm (FIPS 31, p. 11).

2. Physical environment issues in terms of:

- (a) power failure,
- (b) air conditioning failure,
- (c) communications failure,
- (d) ADPE hardware failure (FIPS 31, p. 11) and
- (e) special hazards such as explosives and flammable products in vicinity, unguarded buildings (FIPS 65, p. 8).

3. Compromising emanations (FIPS 31, p. 11).

4. Personnel/access issues such as potential:

- (a) intruders, vandals (FIPS 31, p. 11) malicious destructive acts (FIP 41, p. 13);
- (b) internal theft and abuse (FIPS 31, p. 11), tampering for fraudulent purposes (FIPS 31, p. 9), and deliberate penetrations (FIPS 41, p. 13);
- (c) human errors (FIPS 31, p. 9); and
- (d) non-availability of key personnel (FIPS 31, p. 9).

B. Vulnerabilities including:

1. Input errors - data may be altered, disclosed, lost, or misidentified during input preparation and incorrect, misinterpreted, inconsistent or unreasonable data may be accepted as valid for processing (FIPS 73, p. 10, FIPS 41, p. 12).

2. Open system access - no control over who can use the system (FIPS 73, p. 10; FIPS 41, p. 12).

- 3. Poorly defined information for authorized access-personnel in direct charge of the application may not indicate who should have access to various items of information (FIPS 73, p. 11; FIPS 41, p. 13).**
- 4. Unaudited access to data - if individuals can access data knowing there will be no record of their actions, then they will feel they cannot be held accountable for their acts (FIPS 73, p. 11; FIPS 41, p. 13).**
- 5. Unprotected information - data not protected from unauthorized access, in both on-line and off-line files, such as magnetic tapes; the latter is sometimes accessible by requesting that the tape be mounted (FIPS 73, p. 11; FIPS 41, p. 12).**
- 6. Dial-in access - unauthorized persons may obtain access to the system—especially if remote, dial-in access is allowed (FIPS 73, p. 11; FIPS 41, p. 12).**
- 7. Mistaken processing of data - processing requests may update the wrong data, for example, if the wrong tape is mounted at the wrong time (FIPS 73, p. 11; FIPS 41, p. 12).**
- 8. Operating system flaws - design and implementation errors in operating systems may allow a user to gain control of the system. Once in control, the user can disable controls, erase audit trails, and access any information on the system (FIPS 73, p. 11; FIPS 41, p. 13).**
- 9. Subverting programs - programs containing hidden subprograms that disable security controls. Once in control, user can disable controls, erase audit trails, and access any information in the system (FIPS 73, p. 11; FIPS 41, p. 13).**
- 10. Spoofing - actions can be taken to mislead system personnel or the system software into performing an operation that appears normal, but actually results in unauthorized access (FIPS 73, p. 11; FIPS 41, p. 13).**
- 11. Alteration of data on systems or programs (FIRMR, Section 201-7.103-2).**
- 12. Delay or prevention of ADP operations (FIRMR, Section 201-7.103-2).**

13. Lack of reliability of automated data processing equipment and utilities (FIRMR, Section 201-7.103-2).

14. Eavesdropping - communication lines can be "monitored" by unauthorized terminals to obtain or modify information or to gain unauthorized access to an ADP system (FIPS 41, p. 13).

15. Personnel issues including:

- (a) nonsupervised personnel (FIPS 31, p. 55; FIPS 65, p. 7),
- (b) untrained/inexperienced personnel (FIPS 31, p. 55; FIPS 65, p. 7),
- (c) nonscreened/noncleared personnel (FIPS 31, p. 55),
- (d) nondebriefed terminations (FIPS 65, p. 7).

C. Initial Risks

1. Identify the impact of major failures including:

(a) an analysis of expected losses calculated in dollars or other significant indicators (FIRMR, Section 201-7.103-2) such as (FIPS 73, p. 27):

- (1) extent of inconvenience or hardship to individuals.
- (2) extent of lives lost.
- (3) extent of disruption to the national economy or national security.

(b) an analysis of, but is not limited to, the impact of the following risks (FIRMR, Section 201-7.103-2):

- (1) physical destruction or loss of data and program files (also in FIPS 73, p. 27; FIPS 31, p. 10).
- (2) theft or disclosure of information (also in FIPS 73, p. 7), data confidentiality issues (FIPS 65, p. 9), improper dissemination and careless disposal (FIPS 41, p. 12).
- (3) misuse of ADP system, that is, fraud, vandalism, etc., (see also falsified data, FIPS 73, p. 27; theft of information or assets, FIPS 31, p. 10).
- (4) delay or prevention of ADP operation (see also unavailable data or services, FIPS 73, p. 27).
- (5) lack of reliability of automated data processing equipment and utilities.
- (6) altered or inaccurate data (also in FIPS 73, p. 25).

(c) potential impacts are assessed for every application that will maintain or process sensitive or mission-critical information (implied in FIPS 73, p. 27).

2. Estimate the frequency of major failures in the areas of:

- (a) inaccurate data,
- (b) falsified data,
- (c) disclosed data,
- (d) lost data or programs, and
- (e) unavailable data or services (FIPS 73, p. 27).

3. Estimate the cost of major failures.

(a) Calculate an annual loss expectancy that combines the estimates of the value of potential loss and probability of loss (FIPS 31, p. 11). See prior risk section (2.C.1.,2) for the impact and frequency of failure estimates that the agency should include in its analysis.

(b) Remedial security measures are identified to address significant threats (FIPS 31, p. 13) and vulnerabilities (FIPS 73, p. 25), including measures such as:

- (1) altering the environment (FIPS 31, p. 13),
- (2) erecting barriers (FIPS 31, p. 13),
- (3) improving procedures (FIPS 31, p. 13),
- (4) early detection (FIPS 31, p. 13), and
- (5) contingency plans (FIPS 31, p. 13).

(c) The cost of remedial measures is identified including an identification of the least cost mix of security measures (FIPS 31, p. 13).

Sub-activity

Assess the technical, operational, and economic feasibility of system security alternatives.

Information

A. Technical feasibility assessment—determine whether a proposed alternative(s) system is technically capable of meeting security needs with available technology and methods of operation (FIPS 64, p. 12 for general feasibility requirement, see FIPS 73, pp. 25-26 for addressing security needs).

B. Operational feasibility assessment—determine whether a proposed alternative(s) system is capable of meeting security needs given the operational pattern and resources of the organization, including the “political” environment. (FIPS 64, p. 12 for general operational feasibility requirement, see FIPS 73, pp. 25-26 for assessing operational feasibility of addressing security needs).

C. Economic feasibility assessment. Information on the costs of security for system alternatives are sometimes referred to as either “cost/benefit” or “economic feasibility” assessments (FIPS 64, p. 25). The items are similar for both and appear under the sub-activity below.

Sub-activity

Estimate the security-related costs/benefits of system alternatives.

Information

A. Identify the quantifiable (that is, dollar value) security-related costs of system alternatives including:

1. Non-recurring, capital investment costs of developing, acquiring, and installing security and privacy security controls, such as studies, equipment, facilities, etc. (FIPS 64, p. 35).
2. Recurring costs for operating and maintaining security and privacy security controls such as security training, equipment leasing/rental, maintenance, contractual services, etc. (FIPS 64, p. 36).
3. Annual loss expectancy costs (calculation described in prior risk assessment section) (2.C.1.3) are used in developing system alternative costs (FIPS 73, p. 26).

B. Identify the quantifiable, that is, dollar value and nonquantifiable security-related benefits of system alternatives including:

1. Non-recurring quantifiable cost reductions resulting from system performance monitoring, reduced error rates, and value enhancements such as improved administrative or operational effectiveness (FIPS 64, p. 39).
2. Recurring quantifiable security and privacy benefits of operating and maintaining a system alternative over the system life, such as reduced risk of incorrect processing (FIPS 64, p. 40).
3. Non-quantifiable, intangible benefits of security-related system alternatives, such as reduced risk of incorrect processing (FIPS 64, p. 40) and reduced risk of inaccurate data, and data leakage (industry practice), such as

-
- (a) analysis of "best" and "worst" case scenarios (FIPS 64, p. 40), and
(b) analysis of trade-offs with tangible benefits (FIPS 64, p. 40).
-

3. Identify basic security framework in the selected system alternative.

Sub-activity

Document essential information on the issues and risks (that is, information on security, privacy, and internal controls) present in the system alternative selected (PCMI/PCIE).²

Information

A. Security, privacy, and internal control needs (industry and government practice).

B. Supporting rationale for the disposition of threats, vulnerabilities, and risks inherent in the selected system in terms of cost/benefit tradeoffs; feasibility of addressing, etc. (industry practice).

C. Cost of developing, implementing, and maintaining basic security controls in relationship to the estimated total system development and life cycle cost (industry practice).

Definition Phase

4. Establish quality assurance for security controls development.

Sub-activity

Identify configuration management/change control process.

²The system life cycle matrix and document flowchart found in PCMI/PCIE came from work undertaken by the EDP Systems Review and Security Workgroup of the President's Council on Integrity and Efficiency in coordination with the National Bureau of Standards. This PCIE/NBS work will appear as NBS Special Publication 500-153, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach (expected printing date: March/April 1988).

Information

A. Change control is established for the system (DOD 2168).

B. Change control incorporates the agency's management control process to assure that appropriate administrative, physical, and technical security controls are incorporated into all new applications and into significant modifications to existing applications (OMB A-130, p. III-2). OMB information directs agencies to establish agency-wide procedures/policies for management control of security controls development, and DOD 2167/2168³ and MIL STD 483A require a configuration management plan be developed. Industry practice and DOD 2167/2168 direct that the agencywide standards and procedures be incorporated into the project's configuration management plan.

C. The configuration management process includes controls to change in the security

1. Software (MIL STD 483A, p. 5).
2. Hardware/firmware (MIL STD 483A, p. 5).
3. Interfaces (MIL STD 483A, pp. 5-6, 37-44).
4. Data base (MIL STD 483A, pp. 70, 75).
5. Network (industry practice).

Sub-activity

Identify an internal audit plan.

Information

A. Internal audit plan is drafted (PCMI/PCIE, pp. 66-67).

B. The plan describes auditor involvement in system development. GAO requires auditor review during development to determine that (a) controls have been designed according to management direction and legal requirements, and (b) such controls are operating effectively to provide reliability of, and security over, the data being processed. (See FIPS 73, p. 24; GAO Yellow Book, pp. 57-62, app. I.)

³DOD 2167 (later updated as 2167A) and DOD 2168 are a related set of system/software development guidance. Although throughout this appendix we often cite one or the other, either document usually has comparable information.

C. This plan identifies how the capability to adequately track events during systems operation will be provided to facilitate future audit reviews. (FIPS 73, p. 25; implied should be in audit plan (PCMI/PCIE, pp. 66-67); see also GAO Yellow Book, p. 59, app. I; and TCSEC for audit, p. 96.)

D. The internal audit plan identifies how accepted accounting principles will be complied with for financial applications (FIPS 73, pp. 24-25); implied should be in audit plan (PCMI/PCIE, pp. 66-67); see also GAO Yellow Book, p. 58, app. I.

E. The plan describes the means to assure that controls necessary to protect against loss or serious error will be provided (GAO Yellow Book, p. 60, app. I).

5. Define security requirements.

The information presented in this section could be in either or both a functional or data requirements document. Because functional and data requirements are related, it is difficult to predict which document type will contain which type of information. As a guideline as to where to find specific security information, the purpose of the functional requirements document is "to provide a basis for the mutual understanding between users and designers of the initial definition of the software, including requirements, operating environment, and development plan" (FIPS 38, p. 7). The purpose of the data requirements document is "to provide, during the definition stage of development, a data description and technical information about data collection requirements" (FIPS 38, p. 7). Also note that all security requirements should be explicitly stated so that tests can be designed that will tell if the requirement is satisfied (FIPS 73, p. 30), so each of the security requirements listed below must be specifically and clearly stated. This also means that if there is no requirement, this must be stated.

Sub-activity

Identify fundamental security requirements. Note that TCSEC ("orange book") is the source of these requirements where "TCSEC" appears as the information in this section.

Information

A. Explicit and well-defined security policies enforced by the system that include (TCSEC, p. 3):

1. A set of rules that are used by the system to determine whether a given subject can be permitted to gain access to a specific object (that is, sensitive information).
2. Discretionary access controls to ensure that only selected users or groups of users may obtain access to data (that is, on a need-to-know basis).
3. Marking of every object with a label that reliably identifies the object's sensitivity level (classification, for example), and/or the modes of access accorded those subjects who may potentially access the object.

B. Accountability requirements in terms of:

1. How each access to information is mediated based on who is accessing the information and what classes of information they are authorized to deal with—both identification and authentication security requirements are described (TCSEC, p. 4). Identification is the process whereby a unique identifier (password) is used by a user to enter the system; verification is the process the system uses to “prove” that the user is authorized/is the person associated with the identifier (FIPS 73, p. 13) in terms of (FIPS 73, pp. 14-17):

(a) identification-password, magnetic cards, fingerprints, etc., techniques identified.

(b) authorization-identifies who will have, what modes of access to, which objects (where objects are data objects, executable objects (commands, programs), devices (terminals, printers), storage media (tape reels, disk packs, etc.), transactions, control data within an application, or any combination of the above) including:

(1) delegation of authority-authorization system chosen distinguishes between the right to interact with an object with the right to authorize others to interact with it—these functions are separately controlled.

(2) authorization mechanism is self-protective, that is, cannot be modified by unauthorized personnel.

(3) authorization for confidential/security data is controlled by tagging sensitive objects with confidentiality labels—many different

labels may be used and several labels may be associated with any one object.

(4) types of users are identified and associated with the labels defined in (3) above.

2. Description of how audit information is selectively kept and protected so that actions affecting security can be traced to the responsible party (TCSEC, p. 4), that is, recording of selective events as they occur within a system to identify and trace events involved in data processing or in the use of computer resources (FIPS 73, pp. 17-18) and includes description of (FIPS 73, pp. 18-19):

(a) contents of the journal (nature of the event, identification of all involved elements (people, data, etc.), and information about the event (when, success/failure of event, programs used, etc.).

(b) events to be traced/logged, (that is, what will be "captured").

(c) analysis plan (frequency of review, type of review, how long will be kept/archived (industry practice).

C. Assurance requirements including:

1. Identification of unified collection of hardware and software requirements that perform and enforce security policies, marking, identification, and accountability features (TCSEC, p. 4).

2. Identification of the requirement that the basic hardware and software mechanisms that enforce security policy are themselves not subjected to unauthorized modification or subversion (TCSEC, p. 4).

D. Other performance requirements including:

1. Error tolerance requirements for maintaining error levels within tolerable levels (FIPS 73, p. 30).

2. Availability requirements stated in terms of the maximum length for a service interruption or in terms of frequency of occurrence or as a combination of both factors (FIPS 73, pp. 29-30).

3. Sensitive objects and operations requirements (FIPS 73, p. 29) in terms of:

- (a) the sensitivity and asset value of the data objects (that is, input data, stored data, and output data).
- (b) the security requirements for each data object (or group of related data objects) with respect to the objectives of data integrity, confidentiality, and availability.
- (c) the operations and functions users will perform on data, and where different operations are more sensitive than other operations on the same data, distinguish between the different operations.

Sub-activity

Identify detailed basic control requirements for each application, system interface, and/or each data object (FIPS 73, p. 30; see also OMB A-130, p. III-2 for requirement for agencies to define and approve security requirements prior to acquiring or starting formal development).

Information

Data validation controls requirements—examination of computerized data to determine if it is accurate, complete, consistent, unambiguous, and reasonable (FIPS 73, p. 11) such as:

1. Consistency and reasonableness checks to identify source data and data preparation errors, using techniques like predicted probable value(s) (FIPS 73, p. 12).
2. Validation during data entry—validation routines run against input data before it is processed (FIPS 73, p. 12).
3. Data element dictionary/directory which contains (FIPS 73, p. 13):
 - (a) information to validate data elements, such as information on data element formats and expected relationships between data elements.
 - (b) security authorization specifications to control access to data elements and to aid computer auditing function.
4. Variance detection requirements (mechanism(s) to detect fraud, abuse, misuse, etc. of information and resources (FIPS 73, p. 19)) include:
 - (a) methods/systems to detect suspicious events, such as inspection of journals, physical inspections, interviews, dynamic system monitoring—real-time responses to “trigger-events” (FIPS 73, pp. 20-21).
 - (b) clearly defined responsibilities to investigate security variances once they have been detected (FIPS 73, p. 21).

5. Encryption requirements, that is, transmission and/or storage mechanism to protect information from tampering, disclosure, etc.—primary control to protect data from the hazards of communication systems (FIPS 73, p. 22) mechanism(s) defined for systems containing highly confidential or financial information to be electronically transmitted (FIPS 73, p. 22). Encryption of stored information is sometimes used as it can be less costly than other types of protection; however, encrypted/stored information is not protected from authorized users (FIPS 73, pp. 22-23).

Sub-activity

Results of requirement analysis tools, for example, prototyping and problem statement languages (industry practice) are utilized. Additional guidance on application software prototyping and fourth generation languages is being developed. See, for example, NBS 500-148, May 1987.

Information

Utilize the results of requirements analysis tools to develop security requirements.

6. Select security controls.

Sub-activity

Any new threats, vulnerabilities, or risks resulting from specification of detailed security requirements (see prior step 5) are identified (FIPS 73, p. 27, FIRMR, Section 201-7.103-2). This activity is termed “risk reduction analysis” as it identifies risks on the basis of specific, detailed security requirements and forms the basis for selection of specific security controls. The first risk analysis, conducted during the initiation phase, is based on estimates of risks inherent to general alternative system concepts. If the requirements identified in the prior step are not new, a second risk analysis need not be performed. However, in practice it is unlikely that no new requirements have been added at this point because the definition phase entails defining the specifics of a chosen system on the basis of the general concepts developed during the initiation phase. If the risk analysis (risk reduction in this phase) has been updated, use the list of threats, vulnerabilities, and risks presented in step 2 of this schedule to determine if the updated sections or analysis is complete.

Appendix I
Model of Security in the System Life Cycle
Development Process

Information	Identify and assess the residual risk expected after adopting the security controls (industry practice).
Sub-activity	Identify where security requirements apply in the system.
Information	<p><u>A.</u> Application (OMB A-130, p. III-2).</p> <p><u>B.</u> Application system interfaces including (FIPS 73, p. 29):</p> <ol style="list-style-type: none">1. Define the nature of the interaction between each critical job function, that is, system security planning and control, internal audit, and archival/backup data storage, etc., and the system.2. Identify and define any interfaces to other systems including all critical job functions (or other automated systems) that supply information to the application system, support its operation, or receive its reports.3. Define the responsibilities of individuals who interact with the application system through the interface and identify constraints on the use of each interface that must be enforced if security is to be preserved.4. When the system interacts with other automated systems, determine the degree to which the other system is untrustworthy. <p><u>C.</u> Data base (industry practice).</p> <p><u>D.</u> Operating system/hardware (industry practice).</p> <p><u>E.</u> Telecommunication links (OMB A-130, p. III-3).</p> <p><u>F.</u> Physical environment/installation (OMB A-130, p. III-3).</p> <p><u>G.</u> Administrative/personnel procedures (industry practice).</p>
Sub-activity	Identify the mix of physical, administrative (FIPS 65, p. 21), and technical (FIPS 73, p. 28) security controls that address risks, cost, and security requirements.

Information	<p>A. Major failures identified under section 2.C—Initial Risks. These include the risks of inaccurate data, falsified data, disclosed data, and lost data/programs. A last risk, delay, or prevention of ADP operations is addressed in the following subactivity. Also add any risks identified in the risk reduction analysis, if applicable.</p> <p>B. The cost of each measure, as well as the combined cost of security controls (FIPS 65, p. 21), should be used in the selection.</p> <p>C. Security requirements identified in section 5 (industry practice).</p>
Sub-activity	<p>Develop contingency plans. Contingency plans are a control as they reduce the risk of loss (FIPS 73, p. 22). These plans address availability and continuity of operations requirements—to provide continuity of data processing should normal operations be interrupted. OMB requires contingency plans (OMB A-130, p. III-3), and industry practice suggests development of these plans during the definition phase of development.</p>
Information	<p>A contingency plan contains recovery procedures that guide the return to full and normal data processing capability. See Robert H. Courtney, Jr., “An Economically Feasible Approach to Contingency Planning,” <u>National Computer Security Conference Proceedings</u>, September 15-18, 1986, p. 238.</p>
7. Develop preliminary security test plans.	<p>A preliminary security control evaluation (certification) and accreditation plan is developed. This plan could also include information presented in step 12. If only one test plan exists, use it for both this step and step 12. TCSEC also requires a test plan (p. 106) but does not identify when it should be produced.</p>
Sub-activity	<p>General security objectives, policies, and requirements are described (FIPS 102, pp. 28-29).</p>
Information	<p>A. The application, its boundaries and sensitivities involved (FIPS 102, pp. 28-29).</p> <p>B. Special objectives and restrictions (FIPS 102, pp. 28-29).</p>

C. General schedule restrictions (FIPS 102, pp. 28-29).

D. Security requirements identified (FIPS 102, p. 29). These are the requirements developed by the agency for the system—the list in the test plan should be comprehensive and match the agency’s security requirements. The agency could also list documents to be reviewed to determine requirements (FIPS 102, p. 30).

E. Sources of specific security requirements and policies applicable to the application or existing security documents (FIPS 102, p. 29).

Sub-activity

Resources required and general schedule restrictions to accomplish the certification are estimated and identified.

Information

A. Organization structure and responsibilities for both the evaluation team and other offices (FIPS 102, p. 29); if your agency’s application is critical, an independent body should do the evaluation (FIPS 102, p. 19, TCSEC, p. 86)—use this information if your application is critical).

B. Schedules including:

1. Milestones.

2. Products.

3. Assumptions.

4. Required inputs, such as documentation and briefings (FIPS 102, p. 30).

Sub-activity

Evaluation approach described.

Information

A. Areas of emphasis.

B. Levels of detail.

C. Specific evaluation tasks and techniques, that is, bounding and partitioning of the evaluation work and tasks for each partition. Partitioning/bounding could be different people assigned to: security

management, physical facilities, personnel hardware, software security, service personnel files, internal audit controls, time-resource sharing contingency plan, and use of service bureaus (FIPS 102, pp. 19-20).

D. People to be interviewed.

E. Documents to be reviewed, such as security requirements documents, design documents, security test documents.

F. Test procedures that show:

1. At least 5 system-specific tests that attempt to circumvent the security mechanisms of the system (TCSEC, p. 86).

2. Full, sustained load tests (industry practice).

3. Peak load tests (industry practice).

4. Restart/recovery tests (industry practice).

5. Interface tests (industry practice).

6. Test of training in the use of software/system techniques and procedures are described (industry practice).

Sub-activity

Identifies proposed level of certification and accreditation, that is, C1, C2, etc., (FIPS 102, p. 45; TCSEC, p. 104).

Information

A. Class (D): Minimal Protection (TCSEC, p. 9).

B. Class (C1): Discretionary Security Protection (TCSEC, pp. 12-14).

C. Class (C2): Controlled Access Protection (TCSEC, pp. 15-17).

D. Class (B1): Labeled Security Protection (TCSEC, pp. 20-25).

E. Class (B2): Structured Protection (TCSEC, pp. 26-33).

F. Class (B3): Security Domains (TCSEC, pp. 34-41).

G. Class (A1): Verified Design (TCSEC, pp. 44-52).

8. Design contracts to include security requirements.⁴

Sub-activity	Specifications for the acquisition of ADPE, software, maintenance services, ADP services or support services, and supplies are required to be certified.
Information	The aforementioned specifications are required to be certified by the requiring agency as meeting the agency security needs (FIRMR, Section 201-32.104).
Sub-activity	Solicitation specification shall include, where applicable (FIRMR, Section 201-32.104), the following items to provide security control development quality assurance.
Information	<p><u>A.</u> Agency rules of conduct that a contractor and the contractor's employees shall be required to follow.</p> <p><u>B.</u> A list of the anticipated threats and hazards that have been determined by risk analysis that the contractor must guard against.</p> <p><u>C.</u> A description of the security controls that the user agency specifically requires the contractor to provide.</p> <p><u>D.</u> The standards applicable to the contractual requirement.</p> <p><u>E.</u> The test methods, procedures, information, and inspection system (or the requirement to submit proposals therefore) necessary to verify and monitor the operation of the security controls during contract performance and to discover and counter any new threats or hazards.</p> <p><u>F.</u> The requirement for periodically assessing the security risks involved and advising potential users of the level of security provided.</p>

⁴Means that this security-related activity was not assessed at the nine agencies reviewed.

G. Proposed contractual clauses or provisions, as necessary, to provide for the foregoing.

H. A description of the personnel security requirements.

Sub-activity Evaluation of offers for award, where applicable, will include the following items (FIRMR, Section 201-32.104):

Information A. The adequacy of the proposed security controls program.

B. The presence of security controls, including personnel security requirements.

C. The inclusion in the proposed contract of clauses that appropriately provide for (1) title to security controls designed or developed under the contract, (2) control of publication or disclosure of security controls whether government-furnished or contractor generated, and (3) statement of work adjustments, as necessary, to reflect the contractor's proposal, its evaluation, and the contract negotiation.

Sub-activity Agency monitors contracts (FIRMR).

Information Contract administration should include, where applicable, monitoring of the verification and inspection program for continuing effectiveness of the security control program, including compliance with applicable standards, procedures, and guidelines incorporated into the contract (FIRMR, Section 201-32.104).

Sub-activity The agency procurement request (APR) shall include one of the following statements regarding compliance with the Privacy Act of 1974 (FIRMR, Section 201-23.106-1).

Information A. Equipment or services identified by this request will not be used to operate a system of records on individuals to accomplish an agency function (and/or)

B. Equipment or services identified by this request will be used to operate a system of records on individuals to accomplish an agency mission. All applicable provisions of the Privacy Act have been complied with, including submitting a report of new systems to the Congress and OMB on (date). This means notification in the Federal Register prior to the collection of information (OMB A-130, pp. I-2, I-5).

9. Include approved security requirements in the formal functional baseline (FIPS 101, p. 5; DOD 2167, p. 12).⁵

Documentation produced prior to this step results in the functional baseline—no document review required for this step. The security requirements for the system are frozen at this point, that is, any new requirements cannot be added without backtracking to step 2, consideration of alternatives. During the next phase, design, the configuration management/change control process should actively monitor and evaluate any new requirements. Otherwise, the system could get “out of hand” as new requirements are added, resulting in potentially higher, unanticipated costs and conflicting/contradictory requirements. The tendency, during system development, is for users to continually add or modify requirements.

Design Phase

10. Define security specifications.

“The goal of this phase is to design a solution that satisfies the requirements and constraints, alternative solutions are formulated and analyzed, and the best solution is selected and refined” (FIPS 101, p. 7). OMB A-130, pp. III-2 and III-3 require security specifications for the application to be defined prior to acquiring or starting formal development. A number of different types of information are produced in this phase, which could be located in one or more documents. The information presented in this section is mainly broken-out by the FIPS 38 and FIPS 101 document types. However, information may be “rolled” into one or two documents, as described in FIPS 101, p. 7. Other possible document types include interface, formal, and human engineering specifications (FIPS 102, p. 73). Documents for this activity can include, in varying degrees, information related to the sub-activities presented in this section.

⁵Means that this security-related activity was not assessed at the nine agencies reviewed.

- Design specification—a preliminary design document to identify a high-level solution. (FIPS 101, p. 7; see also TCSEC, pp. 97-98 for a discussion of top-level specifications).
- A detailed design specification—defines and refines the software, that is, algorithms and data to be coded during the next phase (FIPS 101, p. 7).
- Revised requirements specification—design activities may reveal incorrect, infeasible, or ambiguous requirements resulting in the revision of the specification (FIPS 101, p. 7).
- System/subsystem specification—specifies the requirements, operating environment, design characteristics, and program specifications (if desired) for a system or subsystem (FIPS 38, p. 7).
- Program specification—specifies the requirements, operating environment, and design characteristics of a computer program (FIPS 38, p. 7).
- Data base specification—specifies the identification, logical characteristics, and physical characteristics of a particular data base (FIPS 38, p. 7).⁶

Sub-activity

System/subsystem and interface security specifications identify the items listed, as the following information shows.

Information

A. Overall security and privacy requirements imposed on the system/subsystem, or if no requirements are imposed, state this fact (FIPS 38, p. 27; see also TCSEC, p. 97).

B. Interfaces between security control modules are described, if there are distinct security control modules (TCSEC, p. 97).

C. User interfaces that are designed (FIPS 73, p. 31):

1. To be easy to use and understand so that users will not neglect or bypass controls which they view as cumbersome and annoying.
2. To have clear system responses to users that include tactful and helpful error messages—on-line help routines.
3. To include, when possible, appropriate security controls as default options.

⁶The National Computer Security Center will be developing data base and network guidance that could be considered as input to future security specifications.

4. To explain user requests, so that requests that could have unusual serious effects are not executed without the system explaining its interpretation of the request and asking for confirmation.

5. To include restricted user interfaces where interfaces are tailored to meet user requirements and do not include unneeded flexibility, that is, unnecessary access or capabilities.

D. Dedicated, small machines are specified whenever possible to protect sensitive applications and code (rather than use of shared computer facilities/time-sharing (FIPS 73, p. 31).

E. Use of available controls to the fullest extent possible, including:

1. Operating system and facility controls such as user identity verification, authorization for access to system files, journaling of operating system activities, and backup and recovery procedures.

2. Since the security controls of an operating system are not absolutely reliable, the application system uses some data integrity checks to identify if critical data has been altered (FIPS 73, p. 32).

F. Any weak points in the system/subsystem and interface security specifications are identified (implied in FIPS 73, p. 32).

Sub-activity

Identify program, data base, hardware/firmware, and network security specifications (FIPS 38, 73; DOD 1521 B; ISO 7498).

Information

The information for this sub-activity is listed under each individual component.

Program security specifications identify:

A. Security and privacy requirements imposed in the program, the inputs, the outputs, and the data bases; if no requirements are imposed, state this fact (FIPS 38, p. 31).

B. Interfaces with the application system to minimize the danger of users getting unneeded programming capability (FIPS 73, p. 31).

C. Isolation of critical code and system data, when possible (that is, security controls are isolated in modules that have few interactions with the rest of the application software) (FIPS 73, p. 31).

D. All parts of the application system needed to guarantee that the security controls are invoked at the appropriate times (FIPS 73, p. 32).

E. Back-up and recovery mechanisms (FIPS 73, p. 32).

F. Any weak points in the program security specifications are identified (implied in FIPS 73, p. 32). Data base specifications based on preliminary information include:

A. Identification of data base security and privacy restrictions, limitations, and conditions (FIPS 38, p. 35, implied in FIPS 73, p. 31),

B. Identification, labels, and tags designating security and privacy restrictions (FIPS 38, p. 35).

C. Description of all physical access security mechanisms (FIPS 38, p. 35).

D. Any weak points in the data base security specifications are identified (implied in FIPS 73, p. 32).

11. Update security test plan and develop security test procedures.

The items presented in this section build on the items presented in the section on preliminary test plans (see step 7). Both sets of items need to be in the updated test plan.

Sub-activity

On the basis of any revised security requirements or specifications, the test plan is updated, with additional testing procedures identified as necessary (FIPS 101, p. 7).

Sub-activity

Updated test and evaluation plans attempt to demonstrate the system's security software is (FIPS 73, p. 34).

Information	<p><u>A.</u> Meeting its specifications.</p> <p><u>B.</u> Meeting the requirements of the user.</p> <p><u>C.</u> Reliable.</p>
Sub-activity	Final test and evaluation plans are designed.
Information	These plans should provide for testing the system's response to abnormal, unusual, improbable, and illegal circumstances during both data input and data processing (FIPS 73, p. 34).
Sub-activity	Final test and evaluation plans include plans for a variety of static and dynamic testing, including (FIPS 73, p. 35).
Information	<p><u>A.</u> Code review of critical modules or portions of code, which is performed by individuals not involved in the design of programming of the code (static testing).</p> <p><u>B.</u> Penetration studies (which is when a few individuals are challenged to find unknown weaknesses in the security controls (dynamic testing).</p> <p><u>C.</u> Execution of the application system, or portions of the system with test data and comparison of results (dynamic testing).</p> <p><u>D.</u> Flaw hypothesis method testing, whereby analogous security flaws in other systems are tested for existence in this system, (dynamic) (also in TCSEC, p. 86).</p>
12. Include approved security specifications in the formal allocated baseline (FIPS 101, p. 7). ⁷	There probably will not be any documents that specifically identify this step—allocated baseline—because all documents produced during the design phase culminate in this outcome, and will have been reviewed in security activities 10 and 11.

⁷Means that this security-related activity was not assessed at the nine agencies reviewed.

Construction Phase

13. Write security-related code.

Software engineering practices are maintained when developing security-related code. Security-related code includes code that implements security controls, code that performs critical processing (such as check disbursement), and code that accesses critical or sensitive data during execution (FIPS 73, p. 33).

Sub-activity

A program library catalogs and controls access to all versions of program modules as they are being developed, which provides the following types of security controls (FIPS 73, p. 33).

Information

A. Permits only authorized persons access to program modules, that is, list of authorized persons maintained.

B. Records all accesses, especially modifications, to program modules.

C. Associates control data, such as record and byte counts, with program modules, that is, maintains record of control data for modules.

D. Compares current versions of modules with previous versions to identify changed code.

Sub-activity

A high-level programming language is used for code (FIRMR, Section 201-8.107).

Information

Use high-level language for security-related code.

Sub-activity

Structured programming is used, that is, top-down, structured programming (industry practice).

Information

Security-related modules or sections of code are clearly identified and documented (FIPS 73, p. 33).

Sub-activity	Debugging techniques are employed, including (FIPS 73, p. 34).
Information	<p><u>A.</u> Programs run through a preprocessor, that is an automated quality control that checks that program modules meet the coding standards of the project.</p> <p><u>B.</u> Program development tools, such as those that reformat source code, produce cross-reference listings and check syntax errors.</p>
Sub-activity	Configuration management/software modification controls are in place.
Information	Agency configuration management/change control program is involved in writing and documentation of code (see security activity item 4).
14. Perform unit tests on security-related code.	This step could be performed in conjunction with the prior step as part of writing security-related code—debugging techniques described in the prior step could be thought of as part of unit testing. (See steps 16 and 17 for testing.)
Sub-activity	Security-related code is evaluated.
Information	<p><u>A.</u> Peer review of completed code verifies that (FIPS 73, p. 33):</p> <ol style="list-style-type: none">1. Code does not contain any security errors.2. Satisfies all design specifications.3. Is efficient.4. Is easily maintainable. <p><u>B.</u> Walk-through of critical code, a manual process whereby peers/independent reviewers trace the logic of code, is performed (FIPS 73, p. 35).</p> <p><u>C.</u> Critical computations are checked via redundant computation, that is, recalculation of a critical result, checking calculated result</p>

for reasonableness and consistency with other data items, etc. (FIPS 73, p. 34).

15. Include approved security components in the formal developmental baseline (FIPS 73, p. 33).⁸

This is an outcome step—developmental baseline—documentation and practices used in security steps 13 and 14 result in this step. No document review required.

Integration, Installation, and Test Phase

Three different tests are performed during this phase. The tests are sequenced from evaluating relatively small portions of the system to a test of the full system in the “real” environment. The testing sequence involves building the system and assessing how well the system works with each new addition. For example, part of the first test, software configuration assessment, tests the linkages between all the coded units which were individually tested during the construction phase. The next test, system integration, assesses how well the linkages between the hardware, software, and network work. The last test, that is, the acceptance test, adds the factor of the “real” environment and thus the linkage between the full system and the operating environment is assessed. During all of these tests, security controls and issues are assessed.

The same types of testing are done at all three test points—functional and performance testing. In terms of testing security features, functional tests assess protection against human errors or casual attempts to misuse the system. Performance tests, on the other hand, assess factors such as availability, survivability, accuracy, response time, etc. A third type of test, penetration testing, assesses resistance against breaking or circumventing controls, and this test is usually only performed during the last major test—full, stable system, real environment (see FIPS 102, pp. 39-43 for a description of these types of tests).

During testing, the same general items appear under the different tests, that is, functional and performance rated items. Exceptions to this general rule are part of step 16 for network security testing (where items are drawn from the International Organization for Standards and the hardware/firmware component tests (DOD 2167). Another exception is acceptance testing (step 20), where penetration testing is added. The

⁸Means that this security-related activity was not assessed at the nine agencies reviewed.

culmination of all three tests is the security evaluation report, which should contain information on the results specific to security assessments.

16. Conduct tests of security in the configured components.

The three different configured components assessed are the application/software, hardware/firmware, and network, where configured means all pieces are put together, such as all the modules/units of software, and then tested.

Sub-activity

The security features and functions of the configured application/software are assessed.

Information

A. Tests of integrated or aggregated tests of the critical functions (DOD 2167, p. 34). As a note, FIPS 101, p. 13 recommends 100 percent module call.

B. Integrating tests of critical units with any commercially available or government supplied software that will be used in the system (DOD 2167, p. 34). This pertains to "off the shelf" software, such as operating systems that will be used in the final system. Tests of operating systems evaluated by the National Computer Security Center (orange book) are sufficient, that is, they do not need to be repeated by the agency (FIPS 102, p. 25).

C. Functional operation (do controls function properly?) (FIPS 102, pp. 39-43) assessment includes tests of

1. Control operation (for example, do controls work?)

2. Parameter checking (for example, are invalid or improbable parameters detected and properly handled?) such as:

(a) access without a password is disallowed,

(b) invalid passwords are rejected and valid passwords are accepted, and

(c) interface between password function and access authorization function works whereby valid passwords allow proper access and do not allow improper access, and invalid passwords result in proper access restriction.

3. Common error conditions (that is, are invalid or out-of-sequence

commands detected and properly handled?)

4. Control monitoring (for example, are security events, such as errors and file accesses⁹ properly recorded; are performance measurements of characteristics such as resource utilization and response time properly recorded?)

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

6. Other functional tests of critical functions are performed, such as (FIPS 102, p. 41) and

(a) "Through the computer" tests of modules that perform critical functions, such as financial, human safety, etc., algorithms. Several different techniques can be used, such as parallel simulation or tests decks,⁹ and

(b) internal control checks of data reliability using such techniques as foot and balance files.

D. Performance assessments of critical controls, such as (FIPS 102, pp. 41-42):

1. Availability—What proportion of time is the application or control available to perform critical or full services? Availability incorporates aspects of reliability, maintainability, and redundancy. It is especially relevant to applications with denial of service exposures as primary concerns, for example, air traffic control, funds disbursement, etc. Security controls usually require higher availability than other components 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 operations. Restart ("cold start") and recovery testing are useful techniques to assess this part of contingency plans.

3. Accuracy—How accurate is the application or control? Accuracy encompasses the number, frequency, and significance of errors. Some security issues include identity verification accuracy and communication line error handling tests.

⁹Means that this security-related activity was not assessed at the nine agencies reviewed.

4. Response time—(Are response times acceptable? Slow control response time can entice users to bypass the control. Examples of critical response time areas include password and verification processes, and dynamic modifications to security table processes.) Stress testing is a useful technique to test response time, and the next item, throughput. Stress testing can involve attempting to exhaust quota limits for specific resources such as buffers, queues, tables, and ports. Functional operation tests can also be performed under operations stress test conditions, whereby access/verification and normal processing of critical functions is assessed under the high-level load conditions.

5. Throughput—Does the application or control support required usage capacities? Capacity includes the peak and average loading of user and service requests.

E. Any failures to pass tests of critical functions or operations.

F. Tests are performed as described in the test plan and procedures report (implied in FIPS 101 and FIPS 102).

G. Test results are analyzed against security requirements/specifications (DOD 2167, p. 34).

Sub-activity

The security of the configured network is assessed in terms of services, such as listed in the following (International Organization for Standardization 7498/Part 2, pp. 30-31, 34).

Information

A. The peer entity authentication service (an appropriate combination of cryptographically derived or protected authentication exchanges, protected password exchange, and signature mechanisms).

B. The access control service (the appropriate use of specific access control mechanisms).

C. The connection confidentiality service (an encipherment mechanism).

D. The connectionless confidentiality service (an encipherment mechanism).

E. Selective field confidentiality service (an encipherment mechanism).

F. The connection integrity without recovery service (a data integrity mechanism sometimes in conjunction with an encipherment mechanism).

G. The selective field connection integrity service (which protects the integrity of selected fields using a data integrity mechanism, sometimes in conjunction with an encipherment mechanism).

H. The connectionless integrity service (uses a data integrity mechanism sometimes in conjunction with an encipherment mechanism).

I. The selective field connectionless integrity services (which protects the integrity of selected fields by using a data integrity mechanism sometimes in conjunction with encipherment).

J. The data origin authentication service (an appropriate combination of encipherment, signature, and data integrity mechanisms).

K. The non-repudiation with proof of origin service (an appropriate combination of data integrity, signature, and notarization mechanism where signed data units must be stored in the form transferred, together with the presentation context, in order to resolve disputes).

L. The non-repudiation with proof of delivery service (an appropriate combination of data integrity, signature, and notarization mechanisms, where signed data units must be stored in the form transferred, together with the presentation context, in order to resolve disputes).

M. The limited traffic flow security (combines traffic padding with confidentiality service at a lower layer).

N. The connection integrity with recovery service (uses a data integrity mechanism, sometimes in conjunction with an encipherment mechanism).

Sub-activity

Assess hardware/firmware.

Information

The security-related features and functions of the configured hardware/firmware are assessed (DOD 2167, p. 2). Applicable guidance documents were not available during the time of our review. However, if the system is in this phase, the hardware/firmware should be tested before the next security activity—integration testing.

17. Conduct tests of security in the integrated system.

System testing examines the operation and performance of the system as a complete entity, sometimes in a simulated operating environment (FIPS 101, p. 7). System tests conducted in a prototype environment or on “test” hardware qualify as system integration testing. The purpose of this test is to assess the interfaces or linkages between the hardware, software, and network. It is done in a “clean” (prototyped or test) environment so as to control for any extraneous factors that might be introduced in the actual environment, such as software on existing systems with the same name, multiple “unknown” users accessing the system during test, etc. The last test, operating/acceptance test (step 20), assesses these latter factors. Test the security features of the integrated system for the sub-activities of this security activity level.

Sub-activity

Functional operation (do controls function properly?) (FIPS 102, pp. 39-43) assessment include tests of items listed below.

Information

- A. Control operation test (for example, do controls work?).
- B. Parameter checking (for example, are invalid or improbable parameters detected and properly handled?).
 1. Access without a password is disallowed.
 2. Invalid passwords are rejected and valid passwords are accepted.
 3. Interface between password function and access authorization function works whereby valid passwords allow proper access and do not allow improper access, and invalid passwords result in proper access restriction.
- C. Common error conditions (for example, are invalid or out-of-sequence commands detected and properly handled?).

D. Control monitoring (for example, 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?).

E. Control management (for example, do procedures for changing security tables work?).

F. Other functional tests of critical functions are performed, such as (FIPS 102, p. 41):

1. "Through the computer" tests of modules that perform critical functions, such as financial; human safety, etc., algorithms. Several different techniques can be used, such as parallel simulation or test decks.

2. Internal control checks of data reliability using such techniques as foot and balance files.

Sub-activity

Conduct performance assessments of critical controls (FIPS 102, p. 41-42).

Information

A. Availability—What proportion of time is the application or control available to perform critical or full services? Availability incorporates aspects of reliability, maintainability, and redundancy. It is especially relevant to applications with denial of service exposures as primary concerns, for example, air traffic control, funds disbursement, etc. Security controls usually require higher availability than other portions of an application.

B. Survivability—How well does the application or control withstand major failures or natural disasters? "Withstand" includes the support of emergency operations during the failure, back up operations afterwards, and recovery actions to return to normal operations. Restart ("cold start") and recovery testing are useful techniques to assess this part of contingency plans.

C. Accuracy—How accurate is the application or control? Accuracy encompasses the number, frequency, and significance of errors. Some security issues include identity verification accuracy and communication line error handling techniques.

D. Response time—Are response times acceptable? Slow control response time can entice users to bypass the control. Examples of critical response time areas include password and verification processes, and dynamic modifications to security table processes. Stress testing is a useful technique to test response time, and the next item, throughput. Stress testing can involve attempting to exhaust quota limits for specific resources such as buffers, queues, tables, and ports. Functional operation tests can also be performed under operations stress test conditions, whereby access/verification and normal processing of critical functions is assessed under the high-level load conditions.

E. Throughput— Does the application or control support required usage capacities? Capacity includes the peak and average loading of user and service requests.

Sub-activity

Identify any test failures.

Sub-activity

Tests follow test plans and procedures.

Information

Tests are performed as described in the test plan and procedures report (implied in FIPS 101, FIPS 102 and TCSEC).

Sub-activity

Test results are analyzed against security requirements/specifications (DOD 2167, p. 36 and TCSEC, p. 104).

Information

Test is required for the installation and modification of security codes (DOD 2167, p. 34).

18. Install security code and modify as appropriate (FIPS 101, DOD 2167).

No documents need to be reviewed for this step, although any modifications must be incorporated into relevant documents, as appropriate (see security activity 19).

19. Prepare documentation of security controls.

The documentation presented in this section should be based on prior drafts available during the construction phase of development (FIPS 38, p. 6; see also FIPS 105, p. 10 for a discussion of the requirement to produce and revise documents throughout all phases of development). FIPS 105 also presents information on the format, use, and style of documents discussed below. These documents are updated and revised as needed throughout the test phase. The documents should be reviewed at their last revision, or as final documents if the system has completed the acceptance test (security activity 20). We interpret the requirement to prepare the documentation of security controls to be compatible with good practices for quality assurance and software engineering documentation practices. Therefore, the security-oriented aspects of this activity should be included in the basic manuals for systems development, operations, and maintenance. These manuals (FIPS 38 p. 7) are:

- User's manual—sufficiently describes the functions performed by the software in non-ADP terminology, such that the user organization can determine its applicability and when and how to use it. It should serve as a reference document for preparation of input data and parameters and for interpretation of results (see also TCSEC, p. 104).
- Trusted facility manual—description to be provided by the National Computer Security Center and/or DODCI (see also TCSEC, p. 107).
- Operations manual—provides computer operations personnel with a description of the software and of the operational environment so that the software can be run.
- Program maintenance manual—provides the maintenance programmer with the information necessary to understand the programs, their operating environment, and their maintenance procedures.

Sub-activity

We do not provide any sub-activities for this security activity.

Information

The users manual describes (FIPS 38, pp. 38-40):

A. Performance capabilities of the software, including information on inputs, outputs, response time, processing times, error rates, and flexibility and reliability (FIPS 38, p. 38).

B. Security-related data input procedures and requirements of the software such as (FIPS 38, p. 39).

1. Restrictions, for example, priority and security handling, and limitations on what files may be accessed by each type of input transaction.

2. Quality control, for example, instructions for checking the reasonableness of input data, actions to be taken when data appears to be in error, and documentation of errors.

3. Disposition, for example, instructions for retention or release of all sensitive data files received, and other recipients of the inputs.

4. Formats, for example, provide layout forms that explain each entry, its labels (that is, tags or identifiers), controls (that is, header or trailer control data), etc. (where "etc." means describe any input format rules that relate to sensitive fields).

C. Security-related data output procedures and requirements, such as any restrictions on disclosure, dissemination, use of remote devices (FIPS 38, p. 40).

D. Error and recovery procedures and requirements, such as a list of error codes or conditions generated by the software and corrective actions to be taken by the user, including procedures to ensure start-up and recovery capability can be used (FIPS 38, p. 40).

E. File query procedures and requirements regarding use or handling of sensitive files/data (FIPS 38, p. 40).

The Operations Manual provides:

A. Information on emergency or non-routine operations, such as switch over to back-up system and procedures for turnover to maintenance programmers (FIPS 38, p. 43).

B. Information on restart/recovery procedures (FIPS 38, p. 43).

C. Security procedures for running programs through remote terminals (industry practice).

D. Software organization—a diagram showing inputs, outputs, data files, and sequence of operation of the software, with security-critical paths and operations identified (FIPS 38, p. 42).

E. Program inventory where sensitive applications are identified and restrictions described (FIPS 38).

F. File inventory where permanent, sensitive files, and required storage are identified (FIPS 38, p. 42).

G. Run inventory of possible security related-runs listed with the purpose of each run and the progression described (FIPS 38, p. 42).

H. Operating information, such as procedures and contacts for problems with sensitive runs (FIPS 38, p. 42).

I. Information on procedures for sensitive outputs/reports (FIPS 38, 43).

J. Information on restriction level of the manual (that is, operations manual is restricted (industry practice)).

Program Maintenance Manual describes (FIPS 38, pp. 46-47) security areas of:

A. Sensitive programs in the system/subsystem by identifying:

1. Associated title, tag, or label.
2. Functions performed.
3. Problem and solution method (that is, describe the problem to be solved or the program function and the solution method used).
4. Input to program, such as layout, medium used, codes, unit of measurement, format, range of values, or reference a data element directory.
5. Processing features, functions, and purposes, such as:
 - (a) processing logic,
 - (b) linkages,
 - (c) variables and constants,
 - (d) critical/sensitive formulas,
 - (e) error handling provisions,
 - (f) any restrictions or limitations,
 - (g) locations, settings, internal switches, and flags, and

(h) shared storage.

6. Sensitive or restricted output and medium to be used.

7. Sensitive interfaces with other software, data, messages, parameters, conversion requirements, interface procedures, and media used.

8. Sensitive runs, including loading, operating, terminating, and error handling.

B. Procedures for examining and maintaining audit files, as well as giving the detailed audit structure for each type of audit event (TCSEC, p. 17).

C. Operating environment of the system by identifying (FIPS 38, p. 47).

1. Hardware and peripheral equipment required for the operation of the system that uses unusual features or has special restrictions related to security/privacy concerns. (An example would be data transmission devices that have been modified for encryption purposes, or are restricted for certain types of sensitive transmissions.)

2. Unusual features or security/privacy concerns related to the support software such as:

- (a) operating system,
- (b) compiler/assembler, and
- (c) other software.

3. Unusual features or security/privacy concerns related to the data bases.

D. Maintenance procedures for the system including:

1. Programming conventions.

2. Verification procedures (that is, procedures to check the performance of sensitive applications including reference to test data and testing procedures).

3. Error correction procedures (that is, all error conditions, their sources, and procedures for their correction).

4. Special maintenance procedures (that is, information on procedures t

maintain the programs, such as information on periodic purges of data base(s), temporary modifications needed for leap years or century changes, etc.).

Sub-activity

Trusted facility manual contains cautions about functions and privileges that should be controlled when running a secure facility (TCSEC, p. 107).

20. Conduct acceptance test and evaluation of system security (certification)

Sub-activity

Functional operation (do controls function properly?) assessments include tests of the following items (FIPS 102, pp. 39-43).

Information

- A.** Control operation (for example, do controls work?)
- B.** Parameter checking (for example, are invalid or improbable parameters detected and properly handled?) such as
 - 1.** access without a password is disallowed.
 - 2.** invalid passwords are rejected and valid passwords are accepted.
 - 3.** interface between password function and access authorization function works whereby valid passwords allow proper access and do not allow improper access, and invalid passwords result in proper access restriction.
- C.** Common error conditions (for example, are invalid or out-of-sequence commands detected and properly handled?)
- D.** Control monitoring (for example, 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?)

E. Control management (for example, do procedures for changing security tables work?)

F. Other functional tests of critical functions are performed, such as (FIPS 102, p. 41).

1. "Through the computer" tests of modules that perform critical functions, such as financial human safety, etc., algorithms (several different techniques can be used, such as parallel simulation or test decks).

2. Internal control checks of data reliability using such techniques as foot and balance files.

Sub-activity

Performance assessments of critical controls include the following items (FIPS 102, pp. 41-42).

Information

A. Availability—what proportion of time is the application or control available to perform critical or full services? Availability incorporates aspects of reliability, maintainability, and redundancy. It is especially relevant to applications with denial of service exposures as primary concerns, that is, air traffic control, funds disbursement, etc. Security controls usually require higher availability than other portions of an application.

B. 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 operations. Restart ("cold start") and recovery testing are useful techniques to assess this part of contingency plans.

C. Accuracy—How accurate is the application or control? Accuracy encompasses the number, frequency, and significance of errors. Some security issues include identity verification, accuracy, and communication line error handling techniques.

D. Response time—Are response times acceptable? Slow control response time can entice users to bypass the control. Examples of critical response time areas include password and verification processes, and dynamic modifications to security table processes.

Stress testing is a useful technique to test response time, and the next item, throughput. Stress testing can involve attempting to exhaust quota limits for specific resources such as buffers, queues, tables, and ports. Functional operation tests can also be performed under operations stress test conditions, whereby access/verification and normal processing of critical functions are assessed under the high-level load conditions.

E. 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.

Sub-activity

Penetration resistance tests of critical controls includes items listed below.

Information

A. At least five system-specific tests in an attempt to circumvent the security mechanisms of the system (TCSEC, p. 86).

B. A total elapsed time between tests of not less than one month, but not more than 3 months, for a total time spent testing of at least 20 hours (TCSEC, p. 86; FIPS 102, p. 43, suggests no more than 4 months of time should be spent on these tests).

C. An assessment of externally exploitable flaws in internal security functions and interfaces to them such as (FIPS 102, pp. 42-43):

1. Complex interfaces.
2. Change control process.
3. Limits and prohibitions.
4. Error handling.
5. Side effects.
6. Dependencies.
7. Design modifications.
8. Control of security descriptions.

9. Execution chain of security descriptions.

10. Access to residual information.

D. Information to establish confidence in security controls, such as results that (FIPS 102, p. 42):

- 1. Provide an assessment of an application's penetration resistance.**
- 2. Identify difficulties involved in actually exploiting flaws.**
- 3. Provide clear demonstration of flaw exploitability (since it might not be clear from analysis whether, say, an asynchronous timing flaw can be exploited).**

E. Evaluation of hardware (FIPS 102, p. 43), physical, and administrative controls (industry practice).

Sub-activity

The level and type of system security controls are identified. This information should be contained in the final test report that integrates the results of all prior tests (FIPS 102, pp. 45-47).

Information

A. The final test report describes the basic controls/security applications assessed such as:

- 1. General functional characteristics of the application that generally influence its certifiability, that is, presence or absence of user programming (FIPS 102, p. 46).**
- 2. Application boundaries and security assumptions about areas outside the boundary (FIPS 102, p. 46).**
- 3. Hardware, operating system/security kernel configuration (DODCSC, EPL for Trusted Computer Systems, 1985, p. 2).**
- 4. Relationship of controls to security requirements and specifications (DOD 2167, p. 36).**

B. The report summarizes the security evaluation findings and recommendations in the areas of (FIPS 102, pp. 45-46):

1. Application software security controls.
2. Administrative and procedural security controls.
3. Physical security controls.
4. Network security controls (industry practice).
5. Operating system and hardware/firmware security controls (FIPS 102, p. 45), such as (EPL for Trusted Computer Systems and TCSEC, p. 109):
 - (a) level of security provided (that is, C-1, C-2, etc.); and
 - (b) specific areas of security controls, including
 - (1) discretionary access control,
 - (2) object reuse,
 - (3) identification and authentication,
 - (4) audit (that is, journaling capability),
 - (5) system architecture,
 - (6) system integrity,
 - (7) user guide documentation,
 - (8) facility manual (TCSEC, p. 17),
 - (9) test documentation, and
 - (10) design documentation.

C. Describes controls in place, as previously mentioned, and their general roles for protecting assets against threats and preventing exposure (FIPS 102, p. 46).

D. Any failures to pass tests of critical functions/operations. If failure occurs, modifications can be made and the system, that is, all critical code, retested (DOD 2167, p. 37).

E. Includes a certification statement that declares:

1. Compliance with all applicable federal policies, regulations, and standards (OMB 130, p. III-3).
2. Results of tests demonstrate that the installed security controls are adequate for the application (OMB 130, p. III-3).
3. Conformance with security specifications for the system (FIRMR, Section 201-7.106).

4. Any restrictions on use (FIPS 102, p. 47).

5. Any corrective actions that must be undertaken, together with costs and impacts, are recommended and prioritized, along with information to use to evaluate corrections (FIPS 102, p. 47).

21. Accredited system security.

Identify strengths and limitations of system security (FIPS 102).

Information

The accreditation statement declares (FIPS 102, pp. 51-52).

A. The certification report (that is, results of all tests and certification letter described in prior step 20) has been examined.

B. The signing official accepts any residual risks.

C. Any restrictions, which are specifically identified.

D. Any corrective actions that must be taken, which are authorized to be undertaken.

E. Authorization to operate the system/application under the conditions described, that is, restrictions and corrective actions to be taken.

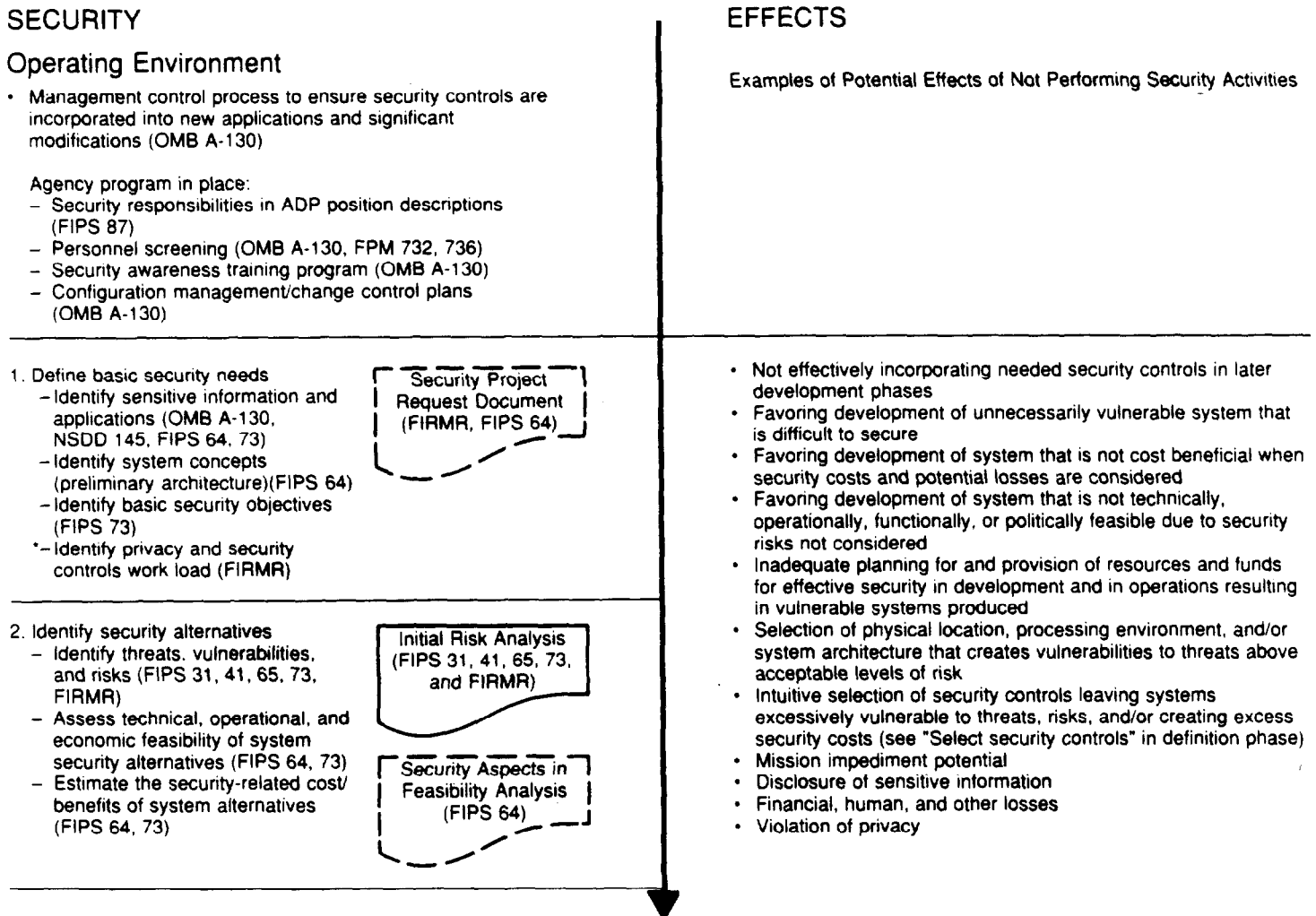
After security activity 21, the product baseline is in place. The product baseline is the sum total of system and security information developed during all preceding steps.¹⁰

¹⁰Means that this security-related activity was not assessed at the nine agencies reviewed.

**Appendix I
Model of Security in the System Life Cycle
Development Process**

Section C: Potential Effects of Not Performing Security Activities During System Development

Figure I.6: Potential Effects of Not Performing Security Activities During System Development: Initiation Phase



Security Project Request Document (FIRMR, FIPS 64)

Initial Risk Analysis (FIPS 31, 41, 65, 73, and FIRMR)

Security Aspects in Feasibility Analysis (FIPS 64)

**Appendix I
Model of Security in the System Life Cycle
Development Process**

3. Identify basic security framework in the selected system alternative
– Provide essential information on security issues and risks (PCMI/PCIE)

Security Areas in Cost/Benefit Analysis (FIPS 64, 73)

Security Areas in System Decision Paper (PCMI/PCIE)

Initiation Phase Completed

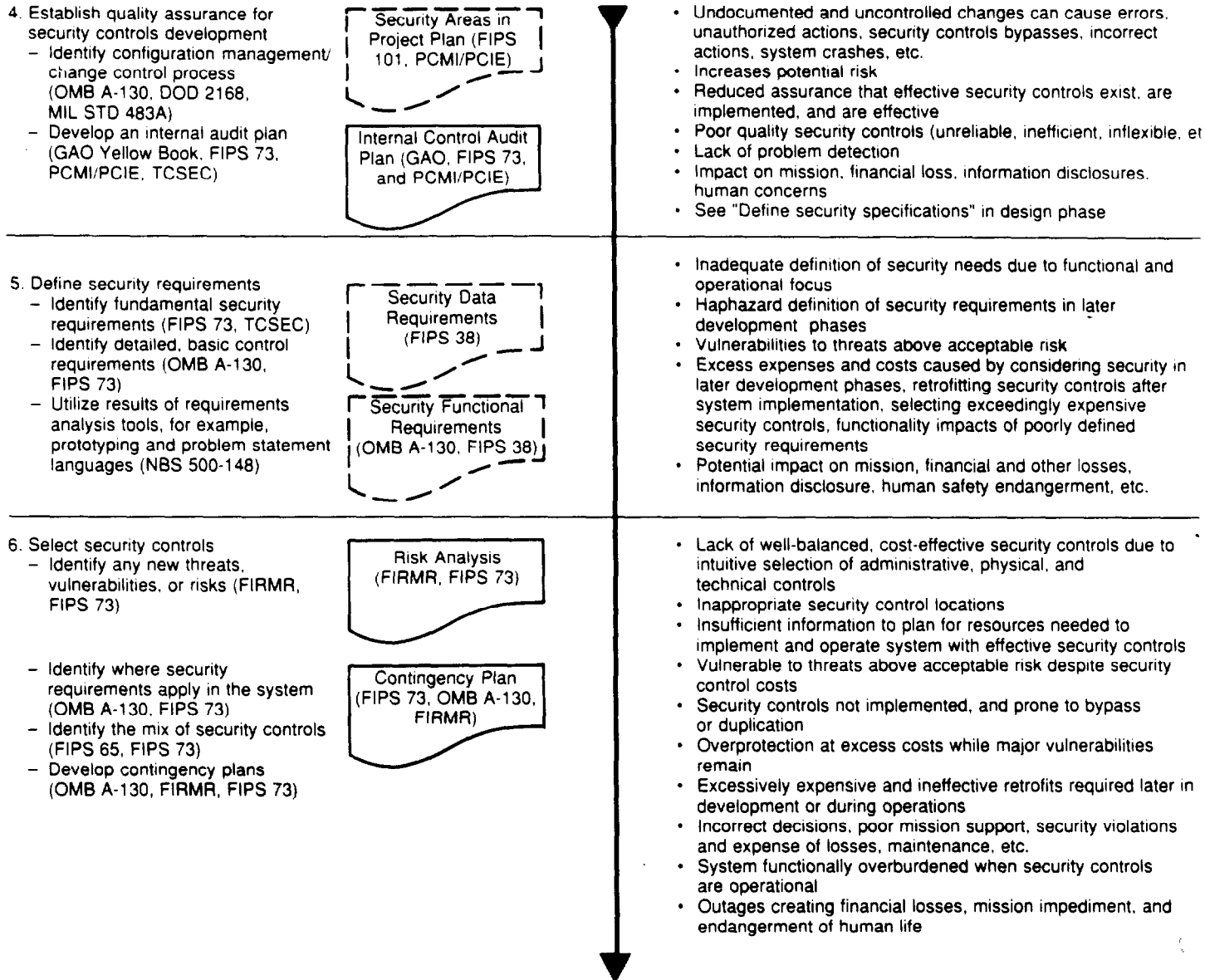


- * Not assessed at the nine agencies reviewed.
- * Acronyms and abbreviations are spelled out in table of contents.

Note: Shared information sources are indicated by a dotted line around the document at the security level, whereas "stand alone" security documents are indicated by a solid line.

**Appendix I
Model of Security in the System Life Cycle
Development Process**

Figure I.7: Potential Effects of Not Performing Security Activities During System Development: Definition Phase



**Appendix I
Model of Security in the System Life Cycle
Development Process**

7. Develop preliminary security test plans
- Identify security objectives, policies, and requirements (FIPS 102, TCSEC)
 - Identify resources and schedule required (FIPS 102, TCSEC)
 - Describe evaluation approach and areas to be tested (FIPS 102, TCSEC)
 - Identify proposed level of certification and accreditation (FIPS102, TCSEC)

Preliminary Security Test Plans
(FIPS 102, TCSEC)

- Insufficient time, resources, and responsibility designations for adequate testing
- Tests performed haphazardly, incompletely, ineffectively, etc., due to poor test cases, failure to test for penetration, quality, integrity, reliability, etc.
- Insufficient dynamic and full load stress testing
- Systems vulnerable to threats above acceptable risk
- Systems that perform and function poorly with security controls operating
- Potential mission impact, and other potential loss, damage, or harm

- *8. Design contracts to include security requirements
- Agency certifies solicitations as meeting security needs (FIRMR)
 - Solicitations provide security controls development quality assurance (FIRMR)
 - Agency evaluates adequacy and presence of security controls in offers (FIRMR)
 - Agency monitors contracts (FIRMR)
 - Procurement request identifies compliance with Privacy Act of 1974 (FIRMR)

RFP(s) and Contract(s)
(FIRMR)

- Contractor failure to perform needed security-related processes and activities during system development
- Production of systems vulnerable to threats above acceptable risk
- Production of overprotected systems at excess cost while vulnerabilities remain
- System does not meet functionality needs when security controls are in operations
- Potential mission impact and other potential loss, damage, or harm

- *9. Include approved security requirements in the formal functional baseline

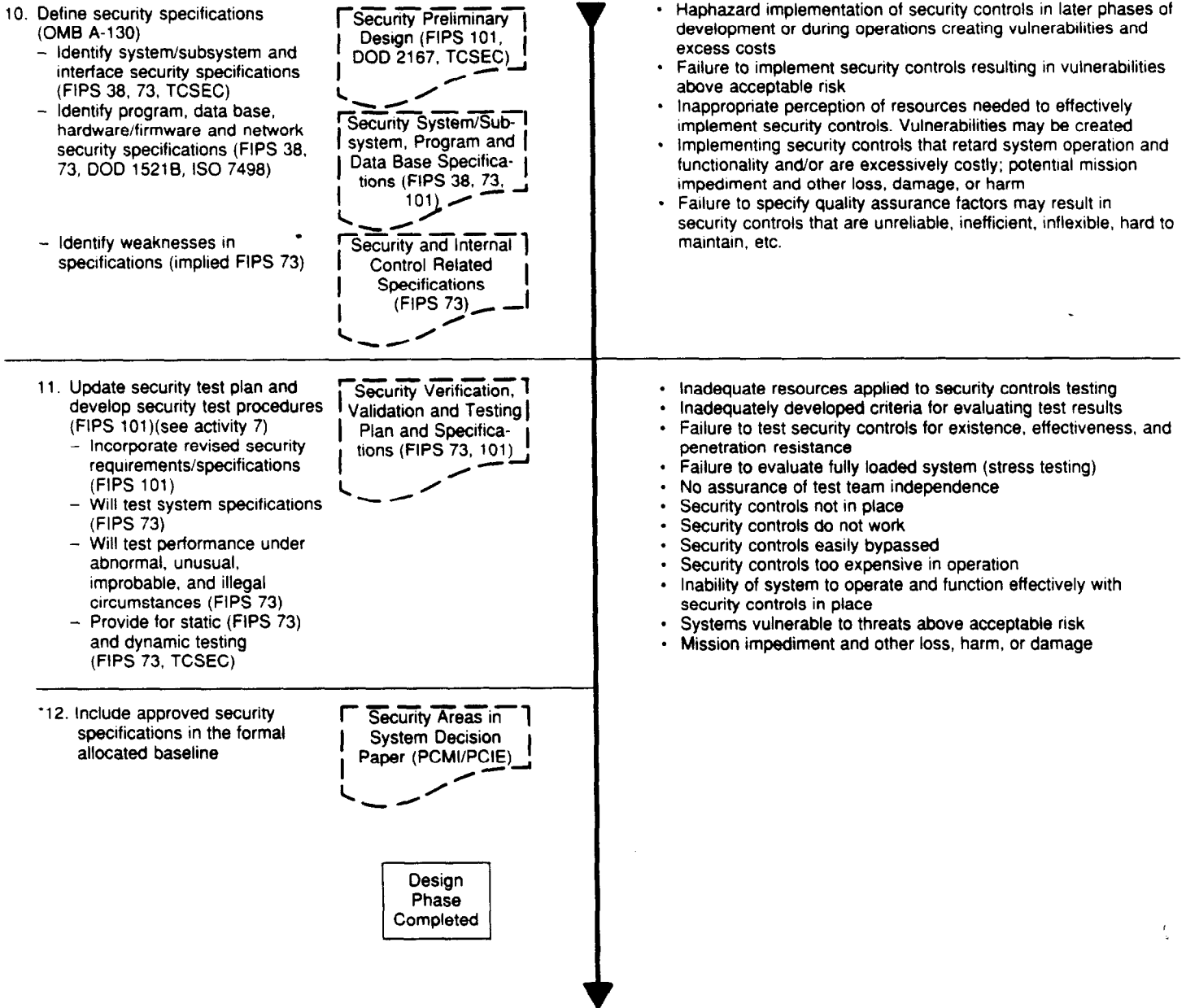
Security System Decision Paper
(PCMI/PCIE)

Definition Phase Completed



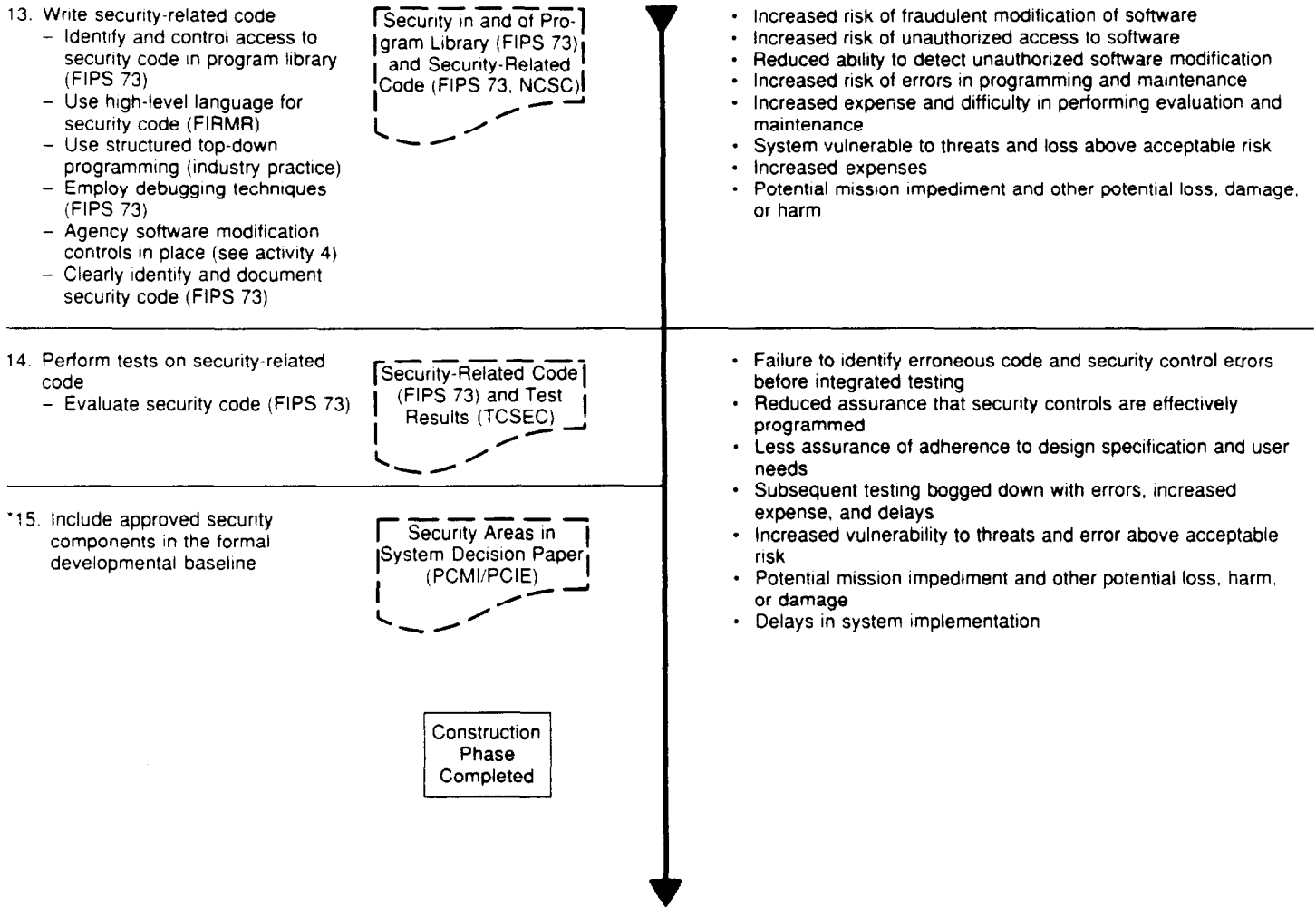
**Appendix I
Model of Security in the System Life Cycle
Development Process**

Figure I.8: Potential Effects of Not Performing Security Activities During System Development: Design Phase



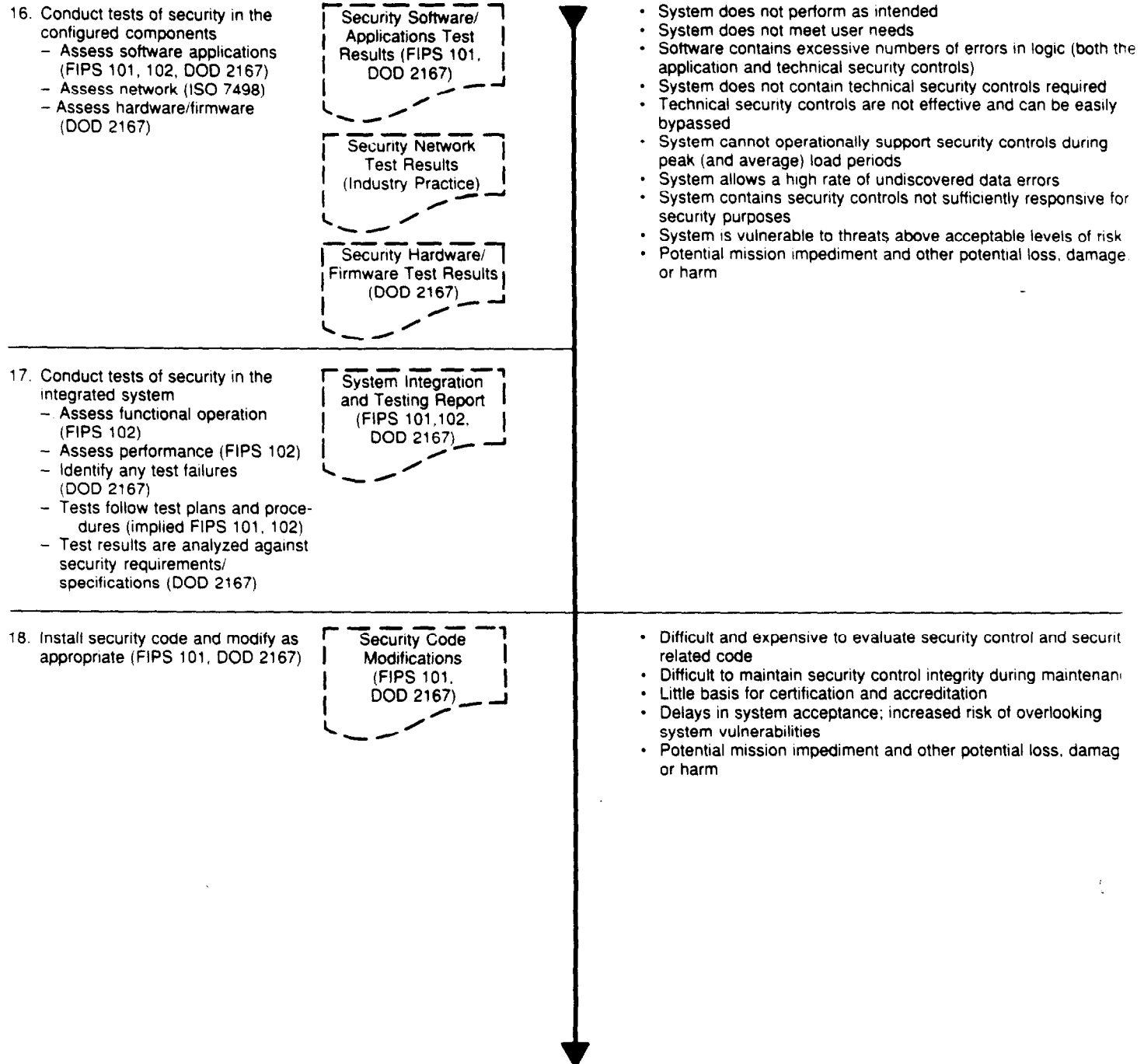
**Appendix I
Model of Security in the System Life Cycle
Development Process**

Figure I.9: Potential Effects of Not Performing Security Activities During System Development: Construction Phase



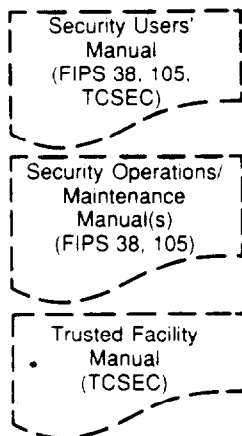
**Appendix I
Model of Security in the System Life Cycle
Development Process**

Figure I.10: Potential Effects of Not Performing Security Activities During System Development: Integration, Installation, and Test Phase



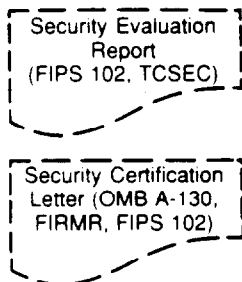
**Appendix I
Model of Security in the System Life Cycle
Development Process**

19. Prepare documentation of security controls



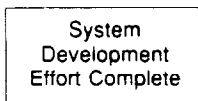
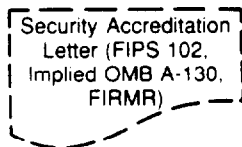
20. Conduct acceptance test and evaluation of system security (certification)

- Assess functional operation (FIPS 102)
- Assess performance (FIPS 102)
- Assess penetration resistance (FIPS 102, TCSEC)
- Identify level and type of system security controls (OMB A-130, FIRMR, FIPS 102, DODCSC, DOD 2167, TCSEC)



21. Accredit system security

- Identify strengths and limitations of systems security (FIPS 102)
- Include all approved security-related elements, for example, tested components, documentation, etc., in the formal product baseline



- System does not perform as intended
- System does not meet user needs
- Software contains excessive numbers of errors in logic (both in application and technical security controls)
- System does not contain technical security controls required
- Technical security controls are not effective and can be easily bypassed
- System cannot operationally support security controls during peak (and average) load periods
- System allows a high rate of undiscovered data errors
- System contains security controls that are not sufficiently responsive for security purposes
- Security tests not integral to system tests
- Technical security controls not supported by complementary administrative and physical security controls and effective management
- Resources not sufficient to make security controls effective
- Excess costs of security retrofit
- System is vulnerable to threats above acceptable levels of risk
- Disclosures of sensitive information
- Potential losses, harm, and damage
- Mission impediment and human safety impacts

Glossary

Access	(1) A specific type of interaction between a subject (for example, user or user process) and an object (for example, data) that results in the flow of information from one to the other. (2) The ability and the means necessary to approach, store, retrieve data, communicate with, or make use of any resource of an ADP system.
Access Control	(1) The limiting of rights or capabilities of a subject (for example, user or user process) or principal to communicate with other subjects, or to use functions or services in a computer system or network. (2) Restrictions controlling a subject's access to an object (for example, data).
Accreditation	The managerial authorization and approval, granted to an ADP system or network, to process sensitive data in an operational environment, 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. Management can accredit a system at a higher/lower level than the certification. If management accredits the system at a higher level than it is certified, management is accepting the residual risk (difference between the levels of accreditation and certification).
Audit Trail	(1) A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports and/or backward from records and reports to their component source transactions. (2) Information collected or used to facilitate a security audit.
Authentication	(1) To establish the validity of a claimed identity. (2) To provide protection against fraudulent transactions by establishing the validity of message, station, individual, or originator.
Availability	(1) The state that exists when required automated services can be obtained within an acceptable period. (2) The property that requires the resources of an open system to be accessible and usable upon demand by an authorized entity.

Baseline	(1) A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures. (2) A configuration identification document or a set of such documents formally designated and fixed at a specific time during a configuration item's life cycle. Baselines, plus approved changes from those baselines, constitute the current configuration identification.
Certification	The technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process, that establishes the extent to which a particular system's design and implementation meet a set of specified security requirements.
Classification	A determination that information requires a specific degree of protection against unauthorized access together with a designation signifying that such a determination has been made. Classification is performed according to a stated security policy.
Communication Link	The physical means of connecting one location to another for the purpose of transmitting and/or receiving data.
Component	A device, consisting of hardware, along with its firmware and/or software, that performs a specific function on a computer communications network. A component is part of a larger system, and may itself consist of other components. Examples include modems, telecommunications controllers, message switches, technical control devices, etc.
Computer Security	The protection of computers and their services from all natural and human-made hazards and provides an assurance that the computer performs its critical functions correctly and there are no harmful side-effects. Includes providing for information accuracy. (See Information Security.)
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Configuration Management	The process that identifies the functional and physical characteristics of an item during its life cycle, controls changes to those characteristics, and records and reports change processing and implementation status. It is thus the means through which the integrity and continuity of the design, engineering, and cost trade-off decisions made between technical performance, producibility, operability, and supportability are recorded, communicated, and controlled by program and functional managers. Configuration management can supply a current description of a developing hardware unit, software unit, system, etc.
Contingency Plan	Describes the appropriate response to any situation which jeopardizes the safety of data or of data processing and communications facilities to a degree that threatens meaningful harm to the organizations supported by those data and facilities.
Continuity of Operations	A system architecture that provides ADP availability within a predefined time period after system failure, as measured by the restart/recovery time (for example, continuous for redundant components, 30 milliseconds, 30 minutes, or 30 hours). (The major security risks during the continuity of operations process include bypassing security controls during restart/recovery operations.)
Data	A representation of facts within a computer or network.
Data Base	An organized collection of data.
Data Confidentiality	The state that exists when data are held in confidence and are protected from unauthorized disclosure.
Data Integrity	(1) The state that exists when computerized data are the same as that in the source documents and have not been exposed to accidental or malicious alteration or destruction. (2) The property that data have not been exposed to accidental or malicious alteration or destruction. (3) In a database system, avoidance of simultaneous update where two concurrently executing transactions, each correct in itself, may interfere with each other so as to produce incorrect results.

Denial of Service	The prevention of authorized access to system assets or services or the delaying of time-critical operations.
Efficiency	The amount of computing resources and code required by a program to perform a function.
Encipherment	See Encryption.
Encryption	The (usually) reversible transformation of data from plain text to ciphertext by a cryptographic device so as to drastically increase the amount of work required to gain access to the information. The purpose is usually to increase the confidentiality of the information, although encryption may be employed as the basis of other security services. Also known as encipherment. (Encryption may be irreversible, in which case the corresponding decryption process cannot feasibly be performed.)
Environment	The aggregate of external circumstances, conditions, and objects that affect the development, operation, and maintenance of a system.
Information	Data that is communicated, interpreted, or processed.
Information Security	Generally considered to be the overall management, procedures, and controls necessary to assure accuracy, integrity, and continuity of operations for an information system.
Integrity	(1) For software quality, the extent to which access to software or data by unauthorized persons can be controlled. (2) For computer, database, and network security, see Data Integrity.
Internal Controls	Includes administrative control and accounting control. Administrative control includes, but is not limited to, the plan of organization and the procedures and records that are concerned with the decision processes leading to management's authorization of transactions. Such authorization is a management function directly associated with the responsibility

for achieving the objectives of the organization and is the starting point for establishing accounting control of transactions. Accounting control comprises the plan of organization, the procedures and records that are concerned with the safeguarding of assets, and the reliability of financial records, and consequently is designed to provide reasonable assurance that:

- a. Transactions are executed in accordance with management's general or specific authorization.
- b. Transactions are recorded as necessary (1) to permit preparation of financial statements in conformity with generally accepted accounting principles, or any other criteria applicable to such statements, and (2) to maintain accountability for assets.
- c. Access to assets is permitted only in accordance with management's authorization.
- d. The recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences. Security controls are considered as supporting selected internal controls. (See Security Controls.)

Journal

An audit trail of data base activities.

Label

(1) One or more characters, within or attached to a set of data, that contain information about the set, including its identification. (2) In computer programming, an identifier of an instruction. (3) An identification record for a tape or disk file. (4) Sensitivity label, a piece of information that represents the security level of an object (for example, data) and describes the sensitivity (for example, classification) of the data in the object.

Maintainability

The effort required to locate and fix an error in an operational program.

Network

A network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include, but are not limited to,

hosts, packet switches, telecommunications controllers, key distribution centers, access control centers, technical control devices, and other components used by the network. Network delimitation is best expressed in terms of the protocol layers. (See Network Architecture.)

Network Architecture

(1) Defines protocols, formats, and standards that different hardware/software must comply with to achieve stated objectives. (2) The International Organization for Standardization provides a framework for defining the communications process between systems. This framework includes a network architecture, which consists of seven layers. The architecture is referred to as the open systems interconnection (OSI) model or reference model. Services and the protocols to implement them for the different layers of the model are defined by international standards. From a systems viewpoint, the bottom three layers support the components of the network necessary to transmit a message. The next three layers generally pertain to the characteristics of the communicating end systems, and the top layer supports the end users. The seven layers are (1) Physical layer: includes the functions to activate, maintain, and deactivate the physical connection and defines the functional and procedural characteristics of the interface to the physical circuit; the electrical and mechanical specifications are considered to be part of the medium itself. (2) Data link layer: Formats the messages and covers synchronization and error control for the information transmitted over the physical link, regardless of the content. "Point-to-point error checking" is one way to describe this layer. (3) Network layer: Selects the appropriate facilities and includes routing communications through network resources to the system where the communicating application is, segmentation and reassembly of data units (packets), and some error correction. (4) Transport layer: Includes such functions as multiplexing several independent message streams over a single connection and segmenting data into appropriately sized packets for processing by the network layer. Provides end-to-end control of data reliability. (5) Session layer: Selects the type of service. Manages and synchronizes conversations between two application processes. Two main types of dialogue are provided: two-way simultaneous (full-duplex) or two-way alternating (half-duplex). Provides control functions similar to the control language in the computer system. (6) Presentation layer: Ensures that messages are delivered in a form that the receiving system can understand and use. Communicating parties determine the format and language (syntax) of messages; translates, if required, and preserves the meaning (semantics). (7) Application layer: Supports distributed applications by

	manipulating information. Provides resource management for file transfer, virtual file and virtual terminal emulation, distributed processing, and other functions.
Notarization	The registration of data with a trusted third party that provides for future recourse to the data and assures accuracy concerning its characteristics such as content, origin, time, and delivery of the data.
Output	Information that has been exported by a trusted computer base.
Password	A private character string that is used to authenticate an identity.
Penetration Testing	The portion of security testing in which the penetrators attempt to circumvent the security features of a system. The penetrators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The penetrators work under no constraints other than those that would be applied to ordinary users or implementors of untrusted portions of the component or system.
Personnel Security	The procedures established to ensure that all personnel who have access to any sensitive information have the required authorities as well as all appropriate clearances.
Physical Security	The measures used to provide physical protection of a system's assets against malicious and accidental attacks. Such measures include the use of locks, guards, and similar administrative mechanisms.
Privacy	(1) The ability of an individual or organization to control the collection, storage, sharing, and dissemination of personal and organizational information. (2) The right to insist on adequate security of, and to define authorized users of, information or systems.

Process	A program in execution. It is completely characterized by a single current execution point (represented by the machine state) and address space.
Program Library	A means of cataloging and controlling access to all versions of program modules as they are being developed. This cataloging and controlling access can either be carried out manually or by automated means.
Protection	Mechanisms and techniques that control access to stored information.
Reliability	The extent to which a system or program can be expected to perform its intended function with required precision.
Resource	Anything used or consumed while performing a function. The categories of resources are time, information, objects (information containers), or processors (the ability to use information). Specific examples are central processing unit time, terminal connect time, amount of directly-addressable memory, disk space, and number of input/output requests per minute.
Risk Analysis	An analysis of system assets and vulnerabilities to establish an expected annual loss or equivalent for certain events based on costs and estimated probabilities of the occurrence, or a ranking of the categories of risk of those events.
Security	Mechanisms and techniques that control access to system assets. Protection is against, for example, unauthorized modification, destruction, denial of service, or theft. Security is an important aspect of broader concepts, such as computer security, information security, and network security. These broader terms address many concerns that are outside the scope of technical and communications security criteria (for example, managerial, physical, and administrative controls). Security is considered as supporting selected internal controls. See Security Controls.

Security Controls	Any action, device, procedure, technique, or other measure that will prevent or diminish the degrading effects on intended system performance from the types of threats mentioned under "Security" above. Security controls are considered as supporting selected internal controls.
Security Policy	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. A complete security policy will necessarily address any concerns beyond the scope of computers and communications.
Security Testing	A process used to determine that the security features of a system are implemented as designed and are adequate for a proposed application environment. This process includes hands-on functional testing, penetration testing, and verification. See also Penetration Testing and Verification.
Sensitive Information	Any information, the loss, misuse, unauthorized access to, or modification of which could adversely affect the national interest, the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act (U.S.C. Title 5, Sec. 552 a), but which has not been specifically authorized under criteria established by executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy.
Sensitivity	The characteristic of an asset (object) that implies its value to the organization using it and the asset's vulnerability to accidental or deliberate threats.
System	An assembly of computer and/or communications hardware, software, firmware, and administrative procedures configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting, and receiving, storing, and retrieving data with the purpose of supporting users.
Threat	A potential violation of system security.

Trusted Computer System	A system that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information.
User	(1) Any person who interacts directly with a computer or network system. This includes both those persons who are authorized to interact with the system and those people who interact without authorization (for example, active or passive wire-tappers). Note that "users" does not include "operators," "system programmers," "technical control officers," "system security officers," and other system support personnel. They are distinct from users and are subject to other managerial and technical requirements. Such individuals may change the system parameters of a computer or network system for example, by defining membership of a group. These individuals may also have the separate role of users. (2) Used imprecisely to refer to the individual who is accountable for some identifiable set of activities in a computer system.
Verification	The process of comparing two levels of system specification for proper correspondence. This process may or may not be automated.

Bibliography

Comptroller General of the United States. "Standards for Audit of Governmental Organizations, Programs, Activities, and Functions." 1981.

General Services Administration. Federal Information Resources Management Regulation, 41 Code of Federal Regulation, chapter 201.

International Organization for Standardization. Reference Model, Security Addendum, Part 2, #7498 (November 1985). The International Standardization Organization proposed network criteria were updated in September 1986 and March 1987 and should also be related to the National Computer Security Center's Trusted Network Interpretation (NCSC-TG-005, Version 1, July 31, 1987).

Office of Management and Budget, Executive Office of the President. Office of Management and Budget Circular Number A-130, December 12, 1985.

Office of Personnel Management, Executive Office of the President. Federal Personnel Manual, chapters 732 and 736.

Office of the President. National Security Decision Directive 145, September 17, 1984). If an automated information system contains information or applications protected under the National Security Decision Directive 145, there is a group of organizations chartered by the Directive to provide guidance. Since the enactment of the Computer Security Act of 1987 (P.L. 100-235), guidance issued under the Directive's authority could be subject to modification or clarification because the act gives the National Bureau of Standards the security standards role for civilian agencies.

President's Council on Integrity and Efficiency. Working Group on Auditing. Matrix Report. (Draft) February 1986.

Note: See U.S. Department of Commerce, National Bureau of Standards. Guide to Auditing for Controls and Security: A System Development Life Cycle Approach. NBS Special Publication 500-153 (expected printing date: March/April 1988). The matrix report is in chapter 2 of this document.

President's Council on Management Improvement and the President's Council on Integrity and Efficiency. Model Framework for Management Control Over Automated Information Systems. (Draft) January 1987.

Bibliography

Note: See U.S. Department of Commerce, National Bureau of Standards. Guide to Auditing for Controls and Security: A System Development Life Cycle Approach. NBS Special Publication 500-153 (expected printing date: March/April 1988).

U.S. Department of Commerce, National Bureau of Standards. "Computer Security Guidelines for Implementing the Privacy Act of 1974." Federal Information Processing Standards. #41 (May 1975).

U.S. Department of Commerce, National Bureau of Standards. Guide to Auditing for Controls and Security: A System Development Life Cycle Approach. Editors/Authors Zella G. Ruthberg, Bonnie Fisher-Wright, James G. Cox, William E. Perry, John W. Lainhart IV, Mark Gillen, Douglas B. Hunt, NBS Special Publication 500-153 (expected printing date: March/April 1988).

U.S. Department of Commerce, National Bureau of Standards. "Guidelines for Automatic Data Processing Risk Analysis." Federal Information Processing Standards. #65 (August 1979).

U.S. Department of Commerce, National Bureau of Standards. "Guidelines for Automatic Data Processing Physical Security and Risk Management." Federal Information Processing Standards, #31 (June 1974).

U.S. Department of Commerce, National Bureau of Standards. "Guidelines for Computer Security Certification and Accreditation." Federal Information Processing Standards. #102 (September 1983).

U.S. Department of Commerce, National Bureau of Standards. "Guidelines for Documentation of Computer Programs and Automated Data Systems." Federal Information Processing Standards. #38 (February 1976).

U.S. Department of Commerce, National Bureau of Standards. "Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase." Federal Information Processing Standards. #64 (August 1979).

U.S. Department of Commerce, National Bureau of Standards. "Guide-

Bibliography

lines for Lifecycle Validation, Verification, and Testing of Computer Software." Federal Information Processing Standards. #101 (June 1983).

U.S. Department of Commerce, National Bureau of Standards. "Guidelines for Security of Computer Applications." Federal Information Processing Standards. #73 (June 1980).

U.S. Department of Commerce, National Bureau of Standards. Guide to Software Conversion Management. Special Publication 500-105 (October 1983).

U.S. Department of Defense. Configuration Management Practices for Systems, Equipments, Munitions, and Computer Programs. Standard 483A (June 4, 1985).

U.S. Department of Defense. Defense System Software Development. Standard 2167A (draft) (April 1, 1987).

U.S. Department of Defense. Software Quality Evaluation. Standard 2168 (April 1985). Department of Defense 2168 was revised on April 1, 1987 (draft).

U.S. Department of Defense. Technical Reviews and Audits for Systems, Equipments, and Computer Software. Standard 1521B (June 1985).

U.S. Department of Defense Computer Security Center (now the National Computer Security Center). Evaluated Products List for Trusted Computer Systems. (1985). This list is updated as new products are added.

U.S. Department of Defense. Department of Defense Trusted Computer System Evaluation Criteria. Updated in December 1985 and related documents (August 1983).



Requests for copies of GAO reports should be sent to:

**U.S. General Accounting Office
Post Office Box 6015
Gaithersburg, Maryland 20877**

Telephone 202-275-6241

The first five copies of each report are free. Additional copies are \$2.00 each.

There is a 25% discount on orders for 100 or more copies mailed to a single address.

Orders must be prepaid by cash or by check or money order made out to the Superintendent of Documents.

United States
General Accounting Office
Washington, D.C. 20548

Official Business
Penalty for Private Use \$300

First-Class Mail
Postage & Fees Paid
GAO
Permit No. G100
