United States General Accounting Office

GAO

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

May 1988

INFORMATION SYSTEMS

Agencies Overlook Security Controls During Development

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

042316

GAO/IMTEC-88-11

GAO

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

Information Management and
Technology Division

B-229223

May 31, 1988

The Honorable Robert A. Roe
Chairman, Committee on Science, Space,
and Technology
House of Representatives

Dear Mr. Chairman:

This report responds to your predecessor's request that GAO, after completing our assessment of operational systems, review computer security practices for automated information systems currently in development. It supplements the testimony GAO gave to the Committee on May 19, 1987 (Information System Security in Federal Civilian Agencies, GAO/T-IMTEC-87-7).

This report includes recommendations to the Directors of the National Bureau of Standards and the Office of Management and Budget. In addition, the report contains recommendations to the heads of agencies.

As arranged with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days after its issue date. We will then send copies to the appropriate House and Senate Committees; Director, National Bureau of Standards; Director, Office of Management and Budget; heads of agencies; and other interested parties.

Sincerely,

fr Daniel C. White

Ralph V. Carlone
Director

Executive Summary

Purpose

Federal agencies have become increasingly dependent in recent years on automated information systems to maintain and process a range of mission-critical, sensitive information. In a request from the Chairman, House Committee on Science and Technology (now the House Committee on Science, Space, and Technology), GAO was requested to review how well civilian agencies were addressing security in their development of mission-critical, sensitive systems. Specifically, GAO was asked to

- determine whether the procedures agencies were using were adequate to assure that appropriate security controls were incorporated in mission-critical, sensitive information systems under development, and
- identify security problems that are common to federal system development efforts.

Background

In 1985, GAO reviewed the security of 25 federal civilian agency automated information systems. GAO identified deficiencies in the controls of those systems that exposed them to abuse, destruction, error, fraud, and waste. Existing federal guidance did not specifically address the procedures required to ensure that appropriate security controls were incorporated into systems. As part of this security review, GAO structured the wide variety of applicable federal policies, standards, and guidelines into criteria that specifically applied to the security aspects of system development. The criteria developed by GAO for this security review proceed from the need to undertake specific security-related activities prior to critical development decisions regarding overall system architecture, detailed system design, system construction, and system testing.

After the GAO review was performed, the Computer Security Act of 1987 (P.L. 100-235) was enacted. The act strengthens the role and responsibility of the National Bureau of Standards for the development and promulgation of computer security standards and guidelines for sensitive information and requires federal agencies to take certain actions in order to strengthen information security.

The National Bureau of Standards plans to issue Special Publication 500-153, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach. The draft of this publication, based in part on material compiled by GAO in this review, contains an evaluation model similar in content to GAO's criteria.

Results in Brief

All nine system development projects GAO reviewed permitted management to make significant decisions without adequate management consideration of potentially important security factors. However, GAO recognizes it may be possible to achieve adequate security controls without using procedures that assure such controls have been achieved. In this regard, it is important to note that GAO assessed the agency procedures used to assure adequate security controls and did not assess the security controls themselves. (See pp. 24-25, 34.)

GAO observed common elements among the problems at the agencies studied. Many of these elements could be traced to the fact that in the early stages of development no agency treated information security as one of the system's integral functional requirements in a manner similar to other user requirements. GAO believes that deficiencies in existing governmentwide policies, standards, and guidelines may significantly contribute to the pervasiveness of the common weaknesses observed.

While inadequate consideration of security control issues during the development stages will not necessarily result in security control weaknesses in the operational system, GAO believes the weight of evidence it obtained, coupled with the magnitude of potential damage, should prompt agencies to take corrective actions. (See pp. 34-36.)

Principal Findings

GAO found significant problems with agency procedures during the first, or initiation, phase of system development. Specifically, agencies did not adequately: (1) determine the systems' information security needs, such as data sensitivity and security objectives, (2) assess the threats, vulnerabilities, and risks to the systems, and (3) identify alternate system security approaches to address risks, and assess and compare the feasibility, costs, and benefits of each alternative. None of the agencies performed both a risk analysis for the specific system concept being used and a feasibility and cost-benefit analysis necessary to effectively evaluate security alternatives. Also, the majority of the agencies in GAO's review either did not define the sensitivity of their information, or did so inadequately.

Additional weaknesses were also evident in subsequent procedures. For example, the nine agencies did not adequately define security requirements to permit implementation of appropriate controls, and three of four agencies that had entered the construction phase did so without developing a security test plan. (See pp. 26-33.)

Recommendations

GAO recommends that

- the National Bureau of Standards, in consultation with the appropriate agencies, perform a comprehensive reassessment and revision of the federal system development standards and guidelines for sensitive information systems under development;
- the Office of Management and Budget revise its existing policies and guidelines for the development of sensitive information systems; and
- the heads of agencies evaluate their current agency policies and procedures to determine if revisions or extensions are necessary to assure that systems are developed with appropriate security controls. (See pp. 36-37.)

Agency Comments

Informal comments on an early draft of GAO's criteria from the President's Council on Integrity and Efficiency, the National Computer Security Center, the Department of Defense Computer Institute, and other entities were generally favorable. (See pp. 22-23.) In providing comments on the draft report, the National Bureau of Standards and the Office of Management and Budget generally agreed with the need to emphasize security in the development of information systems. The National Bureau of Standards provided comments stating that its planned Special Publication 500-153, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach, will address many of the concerns expressed in the draft report.

The Office of Management and Budget said that it will review its governmentwide information security policies to assure that they are consistent with the Computer Security Act of 1987.

GAO informally discussed agency-specific findings with responsible officials at all nine agencies. Most agency officials agreed that the information GAO had gathered was accurate; however, some officials expressed a concern that existing guidance does not require the practices implicit in the GAO model. GAO believes, however, that failure to implement these practices can reduce the assurance of appropriate security controls in a system. (See pp. 37-39.)

Contents

Glossary

Tables

Figure

Abbreviations

ADP	automated data processing
FIPS	Federal Information Processing Standards
FIRMR	Federal Information Resources Management Regulation
GAO	General Accounting Office
GSA	General Services Administration
IMTEC	Information Management and Technology Division
NBS	National Bureau of Standards
OMB	Office of Management and Budget
PCIE	President's Council on Integrity and Efficiency

Chapter 1

Introduction

Many current automated information systems in civilian agencies have been found by us and other organizations to be vulnerable to a range of potential security problems because they do not incorporate appropriate security controls. For example, in a 1985 GAO review of 25 automated information systems at 17 civilian agencies, we testified[1] that each of the systems is vulnerable to abuse, destruction, error, fraud, and waste because of very limited use of security controls, such as risk management and audit trails. A 1986 Office of Technology Assessment review of 142 agency components found similar weaknesses in information security controls and management practices.[2]

Federal automated information systems with inadequate security controls are vulnerable to mission impairment problems that may involve threats to human safety or welfare, compromise of sensitive information, and financial losses. We and others have previously reported on computer system failures related, in part, to problems that could/should have been addressed in development of the system, such as providing for effective computerized controls. For example, in one case we reported that flaws in controls in systems used by the Social Security Administration caused millions of dollars in erroneous payments.[3] We reported further that the Supplemental Security Income Program had provisions for field office personnel to override many of the computerized systems' controls, thus allowing incorrect, incomplete, and erroneous data to be entered into and processed by the computer. In addition, we reported that because of certain limitations of the system, field office personnel had to manually calculate benefit payment amounts when various types of transactions occurred. While the computerized system was programmed to pay these manually calculated benefit payment amounts, the system's automated interface and computational controls were bypassed.

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

[2] U.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).

[3] Flaws in Controls Over the Supplemental Security Income Computerized System Causes Millions in Erroneous Payments (HRD-79-104, Aug. 9, 1979). Solving Social Security's Computer Problems: Comprehensive Corrective Action Plan and Better Management Needed (HRD-82-19, Dec. 10, 1981).

We reported, in another case, that computer security weaknesses in the Community Services Administration helped to make the system exceedingly vulnerable to fraud and abuse.[4] For example, funds available for Community Services' employee payroll and grants were not sufficiently protected. The computer system that was used to process grants and employee payroll lacked descriptive documentation. Programs and changes to them were not properly approved or independently tested. In addition, two basic techniques commonly used in automated payroll systems—record counts and predetermined control totals—were not being used.

In a later GAO report,[5] other related cases have been reported presenting examples of financial loss due, in part, to limited controls in the automated information systems. For example, we cited that it was reported in trade journals that manipulation of input documents at the Social Security Administration's computer processing system resulted in an estimated loss of over $500,000 in disability benefit funds. In another instance of input manipulation, a clerk used a Department of Transportation's computer processing system to steal more than $800,000. In yet another instance, Internal Revenue Service (IRS) employees had prepared fraudulent documents for input to the computer and thereby directed refunds to themselves or others.

Still other examples involve the Department of Agriculture, where at least 30 employees were obtaining unauthorized access to Agriculture's computer and data files. Some used the computer to gain access to and use proprietary data and to make unauthorized and premature disclosure of information considered by Agriculture to be highly sensitive.

The Committee on Government Operations, House of Representatives, reported that credit card information and, in some instances, tax records have been altered or destroyed and the use of computers for theft and fraud has been on the rise over the last five years.[6]

[4] Weak Financial Controls Make the Community Services Administration Vulnerable to Fraud and Abuse (FGMSD-80-73, Aug. 22, 1980).

[5] Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices (MASAD-82-16, Apr. 21, 1982).

[6] Computer Security Act of 1987, Committee on Government Operations, House of Representatives, Rpt. No. 100-153, part 2, p.10 (1987).

The consequences of inadequate controls in government systems are likely to be of increasing importance in the future. The federal government has been expanding its dependence on automated information systems to maintain and process a range of mission-critical, sensitive information. With increased government dependence on information systems and decentralized processing, government automated information systems will be subject to an increased range of vulnerabilities.

Addressing Information Security During System Development Has Advantages

Information security is generally defined as the overall management, procedures, and controls necessary to assure accuracy, integrity, and continuity of operations for an information system. It is generally recognized that the most efficient and effective means to assure that a system contains appropriate security controls is to address information security issues during development.

In this regard, there is a broad spectrum of security controls that can be built into an information system, ranging from the relatively inexpensive and uncomplicated (for example, use of passwords) to the technically challenging and very expensive (for example, A1 certification from the National Computer Security Center). Selection of security controls can significantly affect system cost, complexity, delivery schedule, performance, and functionality. Therefore, it is critical that the design process include determination of what controls are required, and how they will impact system cost, performance, functionality, and delivery schedule.

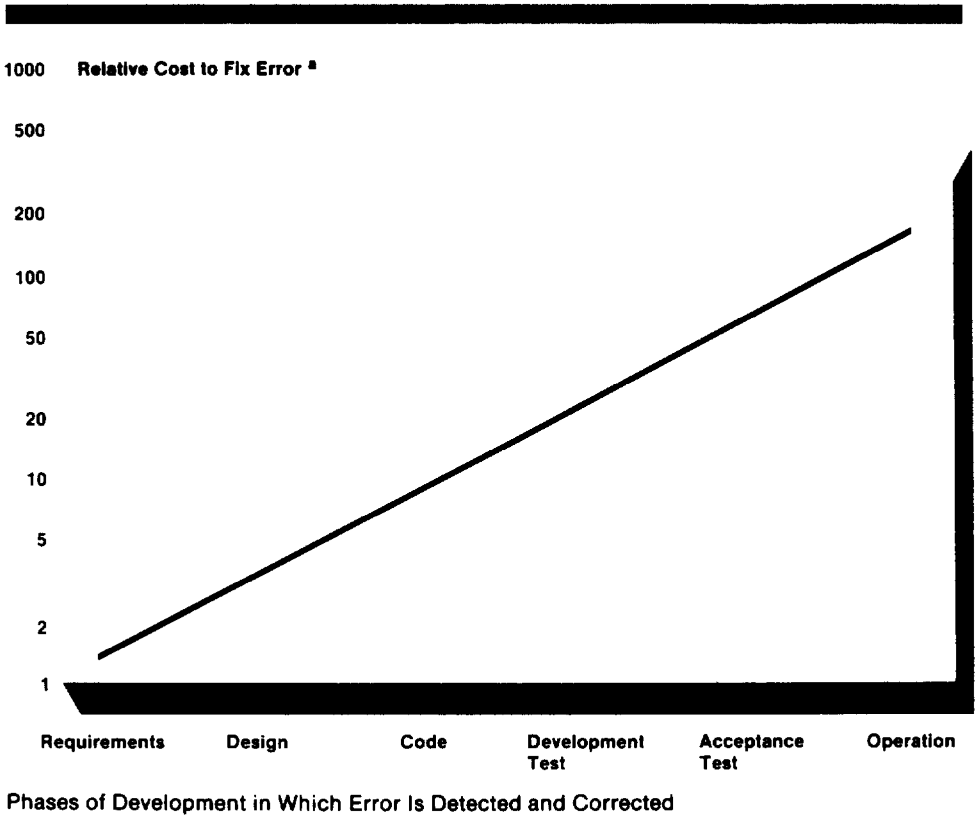
Addressing technical (software-related) security issues, such as access control, early in development or modernization is more effective and less costly than correcting security problems later.[7] For example, it is generally accepted that the cost to change software increases substantially over the life cycle of a system. The magnitude of the increase is illustrated by a 1981 study, reflecting work in a range of software projects, that estimated the cost to address major software problems in large systems in operation at various stages in the system's life cycle. Figure 1.1, adapted from that study, provides a graphic presentation of such costs. This study estimated that for each dollar of software cost incurred incorporating a change related to an error in the requirements phase of an information system, it would on the average require approximately $100 to make an equivalent change in the software after the system was

[7] B.W. Boehm, Software Engineering Economics, (Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1981), pp. 39-41.

operational. Although the 100:1 ratio is obviously a rough estimate and may vary from system to system, circumstance to circumstance, and study to study, we believe that the point is clearly made that it is significantly more costly to correct errors in later phases.

This escalation in cost to address errors as system development progresses makes intuitive sense. When a correction is required after acceptance (system is in operation), more specifications, code, user and maintenance manuals, and training material must be modified. Other elements of the system, designed and implemented without the corrected feature, have to be examined to determine if the correction affects their performance.

Figure 1.1: Increase in Cost to Fix or Change Software During Automated Information System Development



[a]Relative costs as listed here are not dollar figures, but multipliers that are derived from the costs to fix errors in the requirements phase. These multipliers are used to estimate costs to fix errors in subsequent phases.

Source: Adapted from B.W. Boehm, Software Engineering Economics, (Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1981), p.40.

Moreover, in cases where the security features of a system are an important consideration, it may be especially difficult to retrofit security into a system after it is operational. If the functional nature of the system is defined before security concerns are specified, system functional characteristics (such as make payments efficiently) may be inconsistent with appropriate security objectives (such as make correct payments that are free from fraud) and, in some situations, it may be technically and/or economically impossible to correct this problem. For example, certain security features, such as mandatory access control, may be difficult to retrofit into a system after the operational system and application software have been accepted.

Objectives and Scope

The Chairman, House Committee on Science and Technology (now the House Committee on Science, Space, and Technology), requested that we initiate a review of automated information system security for systems under development (see appendix I). This was to be a follow-on to the 1985 GAO review of security in 25 systems[8] already in operation.

On the basis of the Chairman's request and subsequent discussions with his office, our overall objectives for the review were to

- determine whether the procedures agencies were using were adequate to assure that appropriate security controls were incorporated in mission-critical, sensitive automated information systems under development,
- identify any security development problems that are common to the federal system development efforts in general, and
- present a "report card" on the security development practices at nine specifically identified agencies. (This information was presented by GAO at a May 19, 1987 hearing before the House Committee on Science, Space, and Technology, GAO/T-IMTEC-87-7).

Chapter 2 presents our methodological approach to respond to the Chairman's request, with a discussion of how we developed and applied the specific criteria used in our review. This report responds to the first two of the Chairman's overall objectives and presents summary "report cards" for the nine agencies.

[8] Testimony of William S. Franklin, Associate Director, GAO/IMTEC, before the Subcommittee on Transportation, Aviation and Materials of the House Committee on Science and Technology, Oct. 29, 1985.

As requested by the Committee, we did not obtain from the nine agencies we reviewed official agency comments on a draft of this report. However, we informally discussed agency-specific findings with responsible officials at all nine agencies. We obtained formal comments from the National Bureau of Standards (NBS), the Office of Management and Budget (OMB), and the General Services Administration (GSA). We conducted our review in accordance with generally accepted government auditing standards from November 1985 through December 1986.

The agencies and the specific systems under development were selected, with the concurrence of the Committee, among those meeting these criteria: (1) large, mission-critical and/or sensitive systems processing sensitive, but not classified, information and (2) systems for which some auditable development activities had already been performed, ranging from definition stage activities (such as requirements analysis) through system testing. We included in our consideration, and selected for review, nine systems undergoing major development (and intended to be used at least through the 1990s) or modernization. We excluded systems that were primarily in the operation and/or maintenance phases of their life cycles.

In some of the systems selected the system development efforts were too large to review in the time frame of the evaluation and/or were being conducted in modules, where sets of functions to be performed by the system were being developed as individual units. In these cases, we selected a specific module or functional section of the system as our primary basis for review, when this represented a distinct development effort with the full range of development products and activities.

The review was conducted at agency headquarters as well as agency regional offices or contractor locations when the actual system development occurred at locations other than agency headquarters. The agencies and characteristics of the systems selected for review are presented in table 1.1.

Table 1.1: Characteristics of Systems Selected for Review

Agency	System/Subsystem Reviewed	Proposed System Architecture	Estimated Start and End Dates of Development	Phase of Development During Review[a]	Agency Estimate of System Cost[b]
Immigration Naturalization Service	Adjudications Casework System	Centralized processing with remote entry. Mainframe based.	1983-1985	Design[c]	$697,000[d]
Farmers Home Administration	Automated Program Delivery System	Centralized/distributed processing. Mainframe based.	1983-1986	Definition[c]	$7.9 million[e]
U.S. Customs Service	Automated Commercial System/Expanded Selectivity Module	Centralized processing. Mainframe based.	1982-1987	Testing	Total cost estimate not available.
Veterans Administration	Decentralized Hospital Computer Program/Blood Bank and Security Kernel Modules	Distributed processing. Minicomputer based.	1982-1989	Construction	$925 million[f]
Federal Aviation Administration	Advanced Automation System	Distributed/local processing. Mainframe and minicomputer based.	1984-1998	Definition	Over $5 billion
International Trade Administration	Commercial Information Management System	Centralized/distributed processing. Mini and microcomputer based.	1984-1987	Design	$42 million
Social Security Administration	Claims Modernization Program/Release 3.1	Centralized processing with remote terminals. Mainframe based.	1984-1989	Construction	$56.3 million for development
Internal Revenue Service	Automated Examination System	Distributed processing. Mini, micro, and mainframe based.	1982-1988	Definition	Over $1.1 billion
Department of Energy	Strategic Petroleum Reserve System	Centralized processing. Mainframe based.	1985-1987	Construction	$27.9 million for hardware conversion.

[a] We used a five-phased development model, that is: (1) initiation, (2) definition, (3) design, (4) construction, and (5) integration, installation and test.

[b] Agency cost estimates were not reviewed by GAO, and are not necessarily comparable because agencies used different cost bases and some cost estimates do not reflect complete life cycle costs.

[c] First development effort reviewed. Agency terminated the first effort at this phase and is reevaluating system development.

[d] Cost of first development effort at the time of termination.

[e] Estimated cost of first development effort through May 1986; first effort was terminated in July 1986.

[f] Life cycle cost of the decentralized hospital computer program currently planned by the Veterans Administration. This life cycle cost covers fiscal years 1987-1996. For years prior to 1987, GAO reported in Hospital ADP Systems: VA Needs to Better Manage Its Decentralized System Before Expansion (GAO/IMTEC-87-28, July 24, 1987) that cost estimates were incomplete.

[g] Includes a limited amount of hardware necessary for software testing. Does not include total hardware costs.

Chapter 2

Available Criteria Are Sketchy on Security Controls in Automated Information System Development

The Chairman's request for us to review how well civilian agencies were addressing security in their development of mission-critical, sensitive systems required that we make explicit our understanding of how security requirements should influence management decisions in the implementation of a system. Among other things, we had to be able to identify

- the nature of the agency activities that should be undertaken to determine the security threats to and the vulnerability of a proposed automated information system;
- the type of information concerning the major technical and financial factors that could potentially influence the agency's choice of appropriate security controls, given the system's security risks; and
- the relationship between the various security activities and the overall life cycle management framework for the design, construction, and testing of the system as a whole.

Our criteria in this review are based on a considerable body of existing federal direction and guidance[1] that relates to system development and to security controls. However, we found that there is little federal guidance that explicitly addresses the specific issues as noted earlier at a level of detail adequate to serve as criteria in and of itself. In many cases, therefore, we found it necessary to interpret and extend the existing general security-related and system-development-related federal guidance. We extended the applicable guidance to the specific issues involved in the incorporation of appropriate security controls into systems under development. Thus, our findings are based on our amplification of the existing guidance and not necessarily based on a literal reading of guidance.

[1] We generally use the term guidance to refer to the body of federal direction and guidance.

Considerable Federal Guidance Exists on Incorporating Security Controls During Automated Information System Development

Agencies are responsible for assuring an adequate level of security for their systems. To meet this responsibility, the agencies are governed by a framework of governmentwide guidance provided by the National Bureau of Standards (NBS), the Office of Management and Budget (OMB), and the General Services Administration (GSA).

Guidance on federal practices necessary to address information security issues is provided by the Commerce Department's National Bureau of Standards. The Commerce Department is authorized by the Brooks Act and executive orders implementing it to set standards and provide guidance to improve the use of automated information systems in the federa government.

The recently enacted Computer Security Act of 1987 (P.L. 100-235) has strengthened NBS' authority in this area. Specifically, the act assigns to the National Bureau of Standards responsibility for developing and promulgating standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in federal computer systems, drawing on the technical advice and assistance of the National Security Agency where appropriate.[2]

By July 1988, each federal agency is required by the Computer Security Act of 1987 to identify all agency systems in operation and in development that handle sensitive information. Each agency is further required by the act to establish by January 1989, a plan for the security and privacy of each such system that is commensurate with the risk and magni tude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such systems.

In addition, the central management agencies have provided informatior security requirements and guidance to civilian agencies based upon broad statutory authority. OMB has broad authority under the Paperwork Reduction Act to develop and implement policies and guidelines for the security of government information (44 U.S.C. 3504 (a), as amended).

GSA provides guidance for the incorporation of appropriate information security measures in connection with agencies' procurement of automated information systems under authority of the Brooks Act (40 U.S.C

[2] The Computer Security Act of 1987 specifically exempts, from NBS' standard setting, responsibility and authority, certain defense and intelligence activities, as well as systems that are protected through an executive order or act of Congress to be kept secret in the interest of national defense or foreign policy.

759, as amended). GSA's responsibility for incorporating guidance in the Federal Information Resources Management Regulation (FIRMR) includes setting requirements for federal agencies in the area of addressing information security requirements for the management of information resources, including information systems under development. In addition, GSA delineates information security requirements applicable to ADP procurement.

National Bureau of Standards Guidance

The Federal Information Processing Standards (FIPS) provides National Bureau of Standards technical guidelines and standards. These FIPS include suggested federal agency responsibilities and practices to be used to address information security issues for automated information systems under development. A number of the FIPS and Special Publications provide the National Bureau of Standards guidance, some of which is relevant to the incorporation of appropriate security controls in information systems under development.

The FIPS and Special Publications pertinent to information system and security issues that were reviewed as input to our review are listed:

- FIPS PUB 31 "Guidelines for Automatic Data Processing Physical Security and Risk Management," June 1974.
- FIPS PUB 38 "Guidelines for Documentation of Computer Programs and Automated Data Systems," February 15, 1976.
- FIPS PUB 41 "Computer Security Guidelines for Implementing the Privacy Act of 1974," May 30, 1975.
- FIPS PUB 64 "Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase," August 1, 1979.
- FIPS PUB 65 "Guidelines for Automatic Data Processing Risk Analysis," August 1, 1979.
- FIPS PUB 73 "Guidelines for Security of Computer Applications," June 30, 1980.
- FIPS PUB 101 "Guidelines for Lifecycle Validation, Verification and Testing of Computer Software," June 6, 1983.
- FIPS PUB 102 "Guidelines for Computer Security Certification and Accreditation," September 27, 1983.
- Special Publication 500-105 "Guide to Software Conversion Management," October 1983.
- Special Publication 500-148 "Application Software Prototyping and Fourth Generation Languages," May 1987 (and a preceding draft).

OMB Guidance

OMB Circular A-130, issued in 1985, contains the OMB guidance relevant to security in the development of automated information systems. A-130 is an "omnibus" circular intended to summarize OMB guidance across all aspects of information systems policy.

Although not specifically directed to development practices, A-130 contains agency responsibilities and practices that must be considered during system development in the area of information security pertinent to development practices. Specifically, OMB Circular A-130 states that agencies shall assure: (1) that automated information systems operate effectively and accurately; (2) that these systems incorporate appropriate technical, personnel, administrative, environmental, and telecommunications security controls; and (3) the continuity of operations of information systems that support critical/sensitive agency functions.

GSA Guidance

The Federal Information Resources Management Regulation (FIRMR) issued by GSA provides guidance on the acquisition and management of information resources. FIRMR guidance (41 Code of Federal Regulation, Chapter 201) includes security for automated information systems under development. The automated information system development and management requirements in OMB Circular A-130 and FIRMR are similar. For example, FIRMR requires that federal agencies shall establish an adequate security program

> "to ensure automated information system integrity; i.e., a security program that (a) ensures that under all conditions sensitive data is safeguarded from disclosure and protected from unauthorized modification or destruction, (b) provides for operational reliability of the ADP and telecommunications systems, and (c) provides asset integrity for prevention of loss from natural hazards, fire, etc."

Existing Guidance Is Not Adequate for Criteria

We found that some of the existing federal guidance is not sufficiently specific to be used as criteria for our review. Although the applicable NBS, OMB, and GSA guidance was certainly relevant, in most cases we found the guidance to be general in scope and the application to specific system development procedures to be often unclear, inconsistent, or insufficiently detailed.

Several examples illustrate the difficulties we encountered in using existing guidance as the evaluation criteria. The federal guidance is limited in providing a clear and consistent statement of the relationship between the security risk analysis[3] and the various decisions to be made in the development of the overall system. The FIPS do not provide a comprehensive and consistent statement of relationships. For example, neither FIPS 65 nor FIPS 73 clearly indicates the relationship between the security risk analysis and the various decisions to be made in the development of the overall system. However, FIPS 73 does address security issues in system development. In addition, FIPS 102 describes evaluation techniques for certification and includes risk analysis among them. In a similar manner, OMB Circular A-130 mandates the need for risk analysis for computer processing facilities and information applications, however, the circular provides no comprehensive statement of relationships to each of the security related activities necessary for system development decisions.

Certain aspects of information security are apparently omitted from the federal guidance. For example, the need for system cost-benefit and feasibility studies to be performed with sufficient knowledge of the information security controls to be employed is not presented in FIPS 73, OMB A-130, or FIRMR. The FIPS do not provide comprehensive information on alternatives for providing security controls for distributed data bases. In a similar manner, OMB A-130 and FIRMR provide no specific guidance for the need to compare alternative approaches for providing security controls, for example, in telecommunication networks or in end user hardware or software.

Revision of the existing governmentwide regulations, policies, standards, and guidelines pertinent to the assurance of security controls in systems under development—the specific focus of our work—would likely be a process extending over several years. For example, we have previously reported on recommended changes to OMB guidance pertinent to information security and it took over three years for OMB to partially revise the guidance.[4]

[3] Risk analysis is 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.

[4] We recommended in our report, Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices (MASAD-82-18, Apr. 21, 1982) that the Director of OMB revise OMB Circular No. A-71, Transmittal Memorandum No. 1 (July 27, 1978), "Security of Federal Automated Information Systems." OMB partially revised Transmittal Memorandum No. 1 when it issued Circular No. A-130 on Dec. 12, 1985, superseding Circular No. A-71.

Development of Evaluation Criteria

We developed our evaluation criteria in the context of a five-phased model[5] of the system development process. Using this model, we developed the logical relationships between critical decisions in the development process and the information needed to assure the appropriate consideration of security requirements, consistent with existing federal guidance.

It was concluded, after consultation with a number of information security experts, that adequate criteria could be developed from the base of existing federal guidance by: (1) treating security in the early stages of development as an integral "functional requirement" of an information system that should be considered similar to other user requirements and (2) then interpreting and extending existing federal guidance and related disciplines applicable to the analysis, design, construction, and testing of such functional requirements in the automated information system development process.

In doing this we adopted a general standard against which we would measure the adequacy of agency procedures: Agency information system development procedures should provide reasonable, positive, and auditable assurance that cost-effective security controls have been successfully incorporated into the system under development. This standard could equally be applied to any class of a system's functional requirements, for example, the processing of a benefit claim or providing aircraft information to air traffic controllers as well as to security requirements, such as the control of access to sensitive data and applications.

Model of Information Security Activities in the Life Cycle Development Process

We adopted a structured model that viewed the development of an information system as a phased process. We adopted a five-phased model for our analysis that is a compendium of various published models. In doing so, we recognized that particular development efforts might not precisely correspond to the specific steps and sequencing of this model. We believe, however, that the model was sufficiently general to permit the ready identification of the steps undertaken in any particular agency development effort with specific elements of the model.

[5] See the supplement to this report (GAO/IMTEC-88-11S) appendix I, section A, "Model of Security in the System Life Cycle Development Process."

For each of the general systems activities of our model, we identified the specific security activities needed to assure that the major system development decisions are based on an appropriate consideration of security requirements. Table 2.1 summarizes the general system activities and the associated security specific activities. We then developed a "checklist" of the information needed to support knowledgeable decisionmaking for these system activities and to assure that the results of security-related decisions appropriately contributed to system development. The supplement to this report (GAO/IMTEC-88-11S), appendix I contains this checklist as well as the relevant federal document references.

Table 2.1: Information Security Activities in the Life Cycle Development Process

General System Activities	Security Specific Activities
Initiation Phase	
Define and validate need	Define basic security needs
Evaluate alternatives	Identify security alternatives
Select and approve one alternative plan and approach	Identify basic security framework in the selected system alternative
Definition Phase	
Prepare project plan to guide development effort, budget, and schedules	Establish quality assurance for security controls development
Develop basis for design from user requirements	Define security requirements and select security controls
Develop preliminary test plans	Develop preliminary security test plans
Select acquisition strategy commensurate with cost, risk, and urgency of need	Design contracts to include security requirements
Update requirements analysis and establish functional baseline	Include approved security requirements in the formal functional baseline[a]
Design Phase	
Develop detailed design for the system	Define security specifications
Update verification, validation, and testing goals, and plans	Update security test plan and develop procedures
Design a solution that satisfies the requirements and constraints and establish an allocated baseline	Include approved security specifications in the formal allocated baseline[a]
Construction Phase	
Construct from detailed design specifications	Write security-related code
Perform unit tests and evaluate tests results	Perform unit tests on security-related code
Implement detailed design resulting in a system ready for installation and establish a developmental baseline	Include approved security components in the formal developmental baseline[a]

(continued)

General System Activities	Security Specific Activities
Integration, Installation, and Test Phase	
Test system components	Conduct tests of security in the configured components
Validate system performance	Conduct tests of security in the integrated system
Install system	Install and modify security code
Prepare manuals for users, operations, and program maintenance	Prepare documentation of security controls
Perform acceptance test, validate results, and, if necessary, update documentation	Conduct acceptance test and and evaluation of system security (certification)
Accept system and establish a product baseline	Accredit system security and Include all approved security-related elements, for example, tested components, documentation, etc., in the formal product baseline with appropriate security controls in place.[a]

[a] Not assessed for the nine systems reviewed.

Comparability With Other Information Security Approaches

In developing our model, we used as one input an early draft of the Model Framework for Management Control Over Automated Information Systems, prepared by the President's Council on Management Improvement and the President's Council on Integrity and Efficiency in coordination with the National Bureau of Standards.

After developing the criteria, we checked the results for compatibility with other existing agency guidance documents and solicited the opinions of consultants and agency experts.

The agencies and organizations we contacted for assistance informally commented on the merits of our criteria, as incorporated into the model. In general, the consultants and agency experts agreed with the overall form and content of our draft model. Their recommendations principally addressed specific details within the model and alternative groupings of characteristics. For the most part, we adopted their recommendations. Recommendations related to extensions of the model to security areas beyond those subject to our review were not incorporated into the model.

We used the assistance of two expert consultants from the private sector, Dr. D. Elliott Bell, Trusted Information Systems, Inc. and Mr. Frederick G. Tompkins, formerly, ORI, Inc., currently Booz-Allen & Hamilton Inc. We also sought the informal assistance of experts from a number of agencies and organizations. These include the National Bureau of Standards, President's Council on Integrity and Efficiency, National Computer Security Center, and Department of Defense Computer Institute. The comments were generally favorable and included some suggestions for revision of the model. We revised the model as appropriate, to reflect those suggestions received in time for use in our audit work.

Our criteria are generally compatible with the guidance provided by agencies, such as the following agency guidance documents:

- Space and Naval Warfare Systems Command, Computer Security Acquisition Management Guidebook (prepared by Logicon, Inc.: Contract Number N00039-85-D-0105, Task 86-0028, July 1, 1986).
- National Aeronautics and Space Administration, NASA Guidelines for Assuring the Adequacy and Appropriateness of Security Safeguards in Sensitive Applications (prepared by F.G. Tompkins, MITRE: MTR-84W179, Sept. 1984).
- U.S. Department of Commerce, Methodology for Certifying Sensitive Computer Applications, April 1987.

The National Bureau of Standards has informed us that they intend to issue Special Publication 500-153, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach, during the March/April 1988 timeframe. This Special Publication contains a substantially revised version of the PCMI/PCIE model that we had used in the early stages of our effort. Although it differs from our model somewhat in the scope of activities addressed, this revised PCIE/NBS model, which in turn was in part based on materials we compiled in this review, is now very similar in content to our model in those areas that both address.

Assessments of Agency Practices

Our review was based on interviewing officials at nine agencies and obtaining supporting information concerning the security aspects of the applicable systems in development. We used a data collection instrument derived from our criteria to record our findings.

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 the associated security-related factors; and

- these security factors had been arrived at from a base of adequate information concerning the security needs of the system and the range of feasible security alternatives available, as well as any relevant technical and funding limitations.

We classified our assessments into four categories:

Table 2.2: Information Security Assessment Categories

Supports Assurance:	The agency provided evidence that the activity had been performed. We found no significant discrepancies between the results of these activities and our model.
Reduces Assurance (Activity Performed):	The agency provided evidence that the activity had been performed. However, we judged that the results of these activities deviated substantially from our model. This may have been due either to the fact that performance of the activity itself was substantially incomplete or that prerequisites necessary for the meaningful execution of the activity were not present (for example, definition of security specifications without a definition of security requirements).
Reduces Assurance (Activity Not Performed):	Either responsible agency officials stated the security activity was not performed, or we established that there was insufficient documentation to support that the activity had been performed. We judged that this omission represented a substantial deviation from our model.
In Progress (Not Assessed):	The agency was in the process of performing the security activity at the time of our review. We did not have sufficient information to assess this activity.

Limitations of Our Approach

The approach used in this review was developed for the specific purpose of assessing whether agency practices were adequate to assure that appropriate security controls were incorporated in systems under development. In this regard, it is important to note that our assessments are of the agency procedures used to assure the incorporation of adequate security controls and are not assessments of the security controls as such. Such an assessment would not have been feasible as the systems were still under development and not wholly operational at the time of our review.

It should be noted that we developed the model to evaluate information systems under development that will handle sensitive, unclassified information. We recognize that systems handling classified information may have additional information security requirements.

We also recognize that it may be possible to achieve adequate security controls while using procedures that offer no assurance that such controls have been achieved. Thus, a negative assessment is only intended to denote that the development procedures provide inadequate assurance that appropriate security controls will be incorporated into the system and not that the security controls will necessarily be deficient.

NBS and others reviewed our model and suggested additional security activities to be included. However, certain suggestions were received too late to be incorporated in our work.

Chapter 3

Agencies' System Development Procedures Did Not Support Appropriate Security Controls

We observed significant weaknesses in the agencies' system development procedures pertaining to security controls. In particular, agencies' development practices during the first or initiation phase did not comply with our model and therefore lack assurance that they provided an adequate foundation for incorporating security controls commensurate with the threats, vulnerabilities and risk involved. This situation was compounded by agencies not effectively providing reasonable and positive assurance in subsequent development phases that security concerns were appropriately incorporated in the system design, construction, and integration, installation, and test activities.

Initial Development Practices Were Not Adequate

We found significant problems with agency procedures during the first or initiation phase. Specifically, agencies did not adequately

- determine the system's information security needs, such as data sensitivity and security objectives;
- assess the threats, vulnerabilities, and risks to the system; and
- identify alternative system approaches to address risks, and assess and compare the security-related feasibility, costs, and benefits of each alternative.

Information Security Needs Partially Defined

Basic security needs include identifying the sensitivity of the information and associated applications, defining security aspects of the system concepts and identifying the security objectives. Six of the nine agencies arrived at the definition of their overall system requirements without sufficiently considering all three factors establishing basic security needs. Consequently, subsequent developmental efforts addressed only system performance independent of security requirements or needs. For example, three agencies did not attempt to identify whether they did or did not have sensitive data and applications, and three agencies inadequately performed this activity. The agencies that did not identify the data and application sensitivity include the Customs Service, the Immigration and Naturalization Service and the Farmers Home Administration. We view the lack of identification as reducing security assurance because (1) management has no basis for current and future security assessment and (2) developers might not be aware of the need for security controls for mission-critical aspects of the systems.

While agencies did not provide sufficient consideration of all basic security needs, they did, to varying degrees, have some agency practices that supported assurance for security. For example, seven of the nine agencies reviewed adequately identified their security objectives in the areas of data integrity, data confidentiality and ADP service availability—aspects of security that are clearly addressed in existing guidance.

Systems Threats, Vulnerabilities, and Risks Not Adequately Assessed

To determine what security controls should be incorporated into a system, agency management must assess the threats to which the system will be exposed and the vulnerabilities of the system, that is, perform a risk analysis. We found however, that six of the nine agencies did not perform a risk analysis to assess the systems threats and vulnerabilities. For example, the Federal Aviation Administration did not perform a risk analysis for its planned system to support air traffic control, a function where information security may affect mission-critical operations. In another example, a project manager at the Social Security Administration told us that no risk analysis had been performed for its claims processing system because the agency's system development methodology did not include risk analysis procedures.

Two of the remaining three agencies conducted inadequate risk analyses. For example, the Farmers Home Administration assessed risk for its existing loan accounting system and a sample of ADP facilities, but not for its new accounting system design. Only the Department of Energy conducted an adequate risk analysis.

System Approach Selected Without Security Cost-Benefit and Feasibility Assessments

Agencies may not find it possible to incorporate adequate and cost-effective controls if they do not consider the feasibility and cost of incorporating security features when selecting among system alternatives. Nevertheless, we found eight of the nine agencies did not use economic or feasibility assessments when specifying the security features in system alternatives during the initiation phase. For example, the Farmers Home Administration did not identify security alternatives for the three system design options of its proposed accounting system. The Farmers Home Administration did not assess costs and benefits associated with security or the capability of the system alternatives to meet security needs. In contrast, the Internal Revenue Service and its contractor identified three system design alternatives, but they had identical security controls. These security controls were not necessarily feasible for each of the three options. However, the Internal Revenue Service did not perform security feasibility or cost-benefit studies in the initiation phase. Internal Revenue Service officials stated that the agency's experience with security for other systems processing taxpayer information provided sufficient knowledge of feasibility. While we respect Internal Revenue Service experience, we believe that this experience should have been input to security feasibility and cost-benefit studies in the initiation phase.

Summary of Assessment for Initial Development Practices

Table 3.1 displays in summary form our overall assessment of the adequacy of initiation phase activities in supporting the successful achievement of agency mission. The results shown in this table reflect our overall assessment that security development activities in this phase generally did not provide reasonable and positive assurance that appropriate security controls will be successfully incorporated.

Table 3.1: Assessment of Initiation Phase

	Define Basic Security Needs		
Assessment Scale	**Sensitive Information and Applications**	**Overall System Concepts**	**Security Objective**
Supports Assurance	3[a]	5	7
Reduces Assurance (Activity Performed)	3	3	2
Reduces Assurance (Activity Not Performed)	3		
In Progress (Not Assessed)			
Number of Agencies to Which Applicable	**9**	**8[b]**	**9**

	Identify and Assess Security			
		Alternatives	Framework	
Assessment Scale	**Risk Analysis**	**Security Feasibility Study**	**Security Cost/Benefit Study**	**Identify Security**
Supports Assurance	1			
Reduces Assurance (Activity Performed)	2	1	1	6
Reduces Assurance (Activity Not performed)	6	8	8	3
In Progress (Not Assessed)				
Number of Agencies to Which Applicable	**9**	**9**	**9**	**9**

[a] Three agencies adequately identified sensitive information and applications.

[b] Procedure not applied to DOE because the system reviewed was a conversion.

Subsequent Development Procedures Are Inadequate

For the agencies we reviewed, development practices in phases subsequent to the initiation phase, in general, did not support a reasonable and auditable assurance that cost-effective security controls will be successfully incorporated into the system under development. In many cases, we found that deficiencies in phases two through five were related to deficiencies in some preceding phase. Since many essential security activities were not performed in the applicable preceding phase, this could lead to an inadequate understanding of the appropriate security requirements and alternative approaches that could propagate weaknesses in security-related activities throughout the system design, construction, and testing.

Initial Security Problems Were Compounded in Subsequent Development

Because each of the nine system development projects did not fully comply with the security development practices in our model, in the first, or initiation phase of system development, agency management did not have adequate assurance that effective security controls would be successfully incorporated in later phases. Specifically, security requirements for six of the nine systems were determined in the second, or definition phase, without conducting a risk analysis in the initiation phase. Similarly, in the definition phase, all seven agencies that reached the point had insufficient justification for deciding the location of security controls.

These problems carried over from the definition to the third or design phase. Three systems in the design phase had security specifications that reduced assurance due, in part, to a lack of information on the system's security requirements or related, necessary basic information that should have been available in preceding phases.

Subsequent Security Development Activities Not Undertaken

We found that several agencies did not perform subsequent security development activities necessary to provide security assurance: six agencies did not have an audit plan; six agencies did not update or perform risk analyses; three did not identify security controls; and three did not develop security test plans in the definition phase. For example, the Veterans Administration did not identify the security controls selected to protect its blood bank module against identified vulnerabilities. The Social Security Administration, Customs Service, and Veterans Administration entered the construction phase without developing a test plan and procedures for security. Test plans are necessary to ensure comprehensive tests of security controls. The Customs Service was one of the three agencies in our review that had progressed to the testing in the construction phase. However, Customs completed testing without a test plan (design phase) and without security specifications (design phase) against which to compare the controls' capabilities.

Summary of the Assessment for Subsequent Phases

The following tables (tables 3.2 through 3.5) summarize assessments of nine agencies' security activities for .e four remaining development phases. Results for an agency are included up to the point it had reached in system development at the time of our audit. All systems reviewed had at least entered the definition phase of system development. Six of the system development efforts had proceeded to defining design specifications (design phase). Four of the systems had begun construction, and one system was in the integration, installation, and test phase.

Table 3.2: Assessment of Definition Phase

	Establish Quality Assurance Process		Define Security Requiremen
Assessment Scale	**Change Control**[a]	**Internal Audit Plan**	
Supports Assurance	3	2	
Reduces Assurance (Activity Performed)	5	1	9
Reduces Assurance (Activity Not Performed)	1	6	
In Progress (Not Assessed)			
Number of Agencies to Which Applicable	**9**	**9**	**9**

	Select Security Controls			Develop Preliminary Security Test Plan	
Assessment Scale	**Risk Analysis Update**	**Location of Security Controls**	**Mix of Security Controls**	**Contingency Plans**	
Supports Assurance				1	
Reduces Assurance (Activity Performed)		7	3	3	
Reduces Assurance (Activity Not Performed)	6		3	2	[illegible]
In Progress (Not Assessed)	1		1	1	[illegible]
Number of Agencies to Which Applicable	**7**	**7**	**7**	**7**	[illegible]

[a] Change control is the configuration management of proposed systems changes that is performed in a manner to ensure that proposed changes are appropriately analyzed and that only approved changes are made.

Table 3.3: Assessment of Design Phase

Assessment Scale	Define Security Specifications	Update Test Plan and Develop Procedures
Supports Assurance		
Reduces Assurance (Activity Performed)	3	
Reduces Assurance (Activity Not Performed)	3	3
In Progress (Not Assessed)		2
Number of Agencies to Which Applicable	**6**	**5**

Table 3.4: Assessment of Construction Phase

	Write Security-Related Code				Perform Unit Security Testing
Assessment Scale	**Program Library**	**High-Level Language**	**Top Down Programming**	**Debugging Techniques**	
Supports Assurance	2	4		4	
Reduces Assurance (Activity Performed)			4		2
Reduces Assurance (Activity Not Performed)	2				
In Progress (Not Assessed)					1
Number of Agencies to Which Applicable	**4**	**4**	**4**	**4**	**3**

Table 3.5: Assessment of Integration, Installation, and Test Phase

	Test Security in Configured Components			Test Security in Integrated System	
Assessment Scale	**Configured Software Applications**	**Configured Network**	**Configured Hardware/ Firmware**	**Functional Operations**	**Performance of Controls**
Supports Assurance					
Reduces Assurance (Activity Performed)	1			1	
Reduces Assurance (Activity Not Performed)		1	1		1
In Progress (Not Assessed)					
Number of Agencies to Which Applicable	**1**	**1**	**1**	**1**	**1**

(continued)

	Test Security in Integrated System				Update Documentation of Security Controls		
Assessment Scale	**Critical Failures Resolved**	**Testing Follows Test Plans**	**Test Results Analysis**	**Install Security Code**	**User Manual**	**Operations Manual**	**Program Maintenance Manual**
Supports Assurance				1			
Reduces Assurance (Activity Performed)	1				1		
Reduces Assurance (Activity Not Performed)		1	1			1	1
In Progress (Not Assessed)							
Number of Agencies to Which Applicable	**1**	**1**	**1**	**1**	**1**	**1**	**1**

	Conduct Acceptance Test and Evaluation of System Security (Certification)				
Assessment Scale	**Functional and Performance Assessment**	**Penetration Resistance**	**Test Results Report and Evaluation**	**Certification Statement**	**Accredit System Security**
Supports Assurance					
Reduces Assurance (Activity Performed)					
Reduces Assurance (Activity Not Performed)	1	1	1	1	1
In Progress (Not Assessed)					
Number of Agencies to Which Applicable	**1**	**1**	**1**	**1**	**1**

Lack of Appropriate Controls Creates Possible Risks

Systems currently in development at many civilian agencies (and intended to be used at least through the 1990s) are likely to have security deficiencies incorporated in the systems, culminating in inherent risks. Three specific examples of the possible risks at the agencies studied illustrate the potential magnitude of the consequences. First, the Customs Automated Commercial System annually processes transactions representing about $16 billion of import duties, tariffs, and fines. The Automated Commercial System stores sensitive cargo inspection data that if disclosed to unauthorized people, could compromise Customs' ability to collect import duties and tariffs and prevent the smuggling of contraband. Second, the Immigration and Naturalization Service planned to use its Adjudications Casework System to process applications of aliens seeking approval to enter and reside in this country legally. Without proper controls, this system could be used to provide legal status to aliens who otherwise would not qualify. Third, the Federal Aviation Administration's Advanced Automation System will be processing in-flight data for aircraft flying under instrument flight rules or visual flight rules. Security controls could be viewed in a broad sense as protecting the integrity of flight data. Therefore, flight safety degradation resulting from discontinuities in system availability may be considered as a potential security risk.

Since the Automated Commercial System and the Advanced Automation System will be operating as the next generation of automated information systems, we are concerned that these potential security problems may be unresolved for the life of the systems.

Conclusions, Recommendations, and Our Evaluation

Conclusions

Prior reviews have found that many automated information systems currently in operation at civilian agencies are subject to a range of potential security problems because they do not incorporate appropriate security controls. Our findings in this report show that such vulnerability could be minimized or avoided if agencies were to follow system life cycle practices such as those contained in our model or the PCIE/NBS model (to be issued in NBS Special Publication 500-153, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach).

Agency Development Practices Do Not Assure That Adequate Security Controls Are Incorporated

At each of the nine agencies we studied we found that the development procedures did not provide a reasonable, positive, and auditable assurance that cost-effective security controls have been successfully incorporated into the system under development. We found problems that were common among the agencies studied. No agency treated security in the early stages of development as one of the system's integral functional requirements in a manner similar to other user requirements, when making major decisions affecting the development of the overall system. Consequently, all nine system development projects reviewed arrived at their overall system architecture and functional requirements without adequate management consideration of security issues that might have influenced these basic system development decisions. In particular, we judged that no agency has performed risk analyses, feasibility, and cost-benefit studies adequately to assure the appropriate consideration of security controls. These problems were compounded in subsequent development activities.

Sensitive Systems May Have Significant Security Flaws

Without adequate assurance that appropriate security controls have been incorporated in the systems under development, agency management cannot determine whether significant security flaws may exist in these systems, which expose the agency to loss of assets, system fraud, and abuse. Three specific examples of the possible risks at the agencies studied illustrate the potential magnitude of the consequences. First, the Customs Automated Commercial System stores sensitive cargo inspection data that, if disclosed to unauthorized people, could compromise Customs' ability to collect import duties and tariffs and prevent the smuggling of contraband. Second, the Immigration and Naturalization Service planned to use its Adjudications Casework System to process applications of aliens seeking approval to enter and reside in this country legally. Without proper controls, this system could be used to provide legal status to aliens who otherwise would not qualify. Third, the Federal Aviation Administration's Advanced Automation System will be processing in-flight data for aircraft flying under instrument flight rules or visual flight rules, and would be subject to impaired flight data availability.

Problems With Federal Guidance Contribute to Lack of Assurance

We believe that deficiencies in existing governmentwide policies, standards, and guidelines may significantly contribute to the existence of common weaknesses in the security aspects of agency system development practices. We found that the existing regulations, policies, standards, and guidelines were not an adequate basis for evaluating whether specific practices would assure the incorporation of adequate security controls. Informal agency comments suggest that agency management finds them an equally unsuitable basis for managing the security aspects of a system development effort.

NBS will begin to address these issues in its planned Special Publication 500-153, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach. This document is based on concepts of sound system development practices very similar to those endorsed in our model. It is written, however, as a guide to auditing the system development process and does not contain explicit guidance to the systems developers and their management. Most importantly, it is not a standard and is not compulsory and binding because Special Publications are not specifically recognized as FIPS Standards or Guidelines.

We are concerned that a comprehensive revision of the existing governmentwide regulations, policies, standards, and guidelines pertinent to the assurance of security controls in systems under development would likely be a process extending over several years. For example, we have previously reported on recommended changes to OMB guidance pertinent to information security and it took over 3 years for OMB to partially revise the guidance.[1]

[1] We recommended in our report, Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices (MASAD-82-18, Apr. 21, 1982) that the Director of OMB revise OMB Circular No. A-71, Transmittal Memorandum No. 1 (July 27, 1978), "Security of Federal Automated Information Systems." OMB partially revised Transmittal Memorandum No. 1 when it issued Circular No. A-130 on Dec. 12, 1985, superseding Circular No. A-71.

Possibility of Governmentwide Problem

The results of this review, along with results of our prior reviews, suggest that

- poor security-related system development practices are common throughout civilian government,
- these practices have significantly contributed to the existing state of automated information system security in these agencies, and
- many, if not most, of the civilian agency systems currently in development will be similarly affected.

Our review adds credence to these concerns. All nine agencies reviewed were found to have deficiencies in their system development practices, which increase the risk that these systems being developed will have inadequate security controls. The governmentwide guidance, which governs these practices at the nine agencies as well as at all other civilian agencies, was found to be significantly weak in this area.

We believe that the weight of evidence obtained in this review, when coupled with the magnitude of the potential damage (see the supplement to this report, appendix I: section C), ought to be of significant governmentwide concern and motivate corrective actions.

Recommendations

We recommend that the National Bureau of Standards, pursuant to its responsibilities under the Computer Security Act of 1987 and in consultation with the appropriate agencies, perform a comprehensive reassessment and revision of the system development standards and guidelines needed by agencies to assure cost-effective protection of sensitive information in federal computer systems under development. This effort could be based, at least in part, upon the concepts of good system development practices underlying the Guide to Auditing for Controls and Security: A System Development Life Cycle Approach that is planned for release in the March/April 1988 timeframe by the National Bureau of Standards as Special Publication 500-153.

We recommend that the Office of Management and Budget, consistent with its broad authority under the Paperwork Reduction Act, revise its existing policies and guidelines to ensure appropriate management involvement in security-related decisions governing the development of sensitive information systems.

We recommend that the heads of agencies evaluate their current agency policies and procedures governing the development of sensitive information systems to determine if revisions or extensions are necessary to assure that systems are developed with appropriate security controls. The agencies may find the forthcoming National Bureau of Standards Special Publication 500-153 useful in this analysis. We further recommend that heads of agencies review sensitive information systems that are currently under development to evaluate to what extent a sound security foundation has been laid for their implementation. Consideration of these evaluations should be included in the formulation of agency information security plans required by the Computer Security Act of 1987.

Agency Comments and Our Evaluation

We received formal comments on a draft of this report from NBS, OMB, and GSA. At the Committee's request, we did not obtain official agency comments on a draft of this report from the nine agencies we reviewed. We did, however, informally discuss agency-specific findings with responsible officials at all nine agencies.

Most agency officials agreed that the information we had gathered was accurate. Some agency officials, however, expressed a general concern at our use of a model that went beyond mandatory federal criteria. We recognize that existing guidance does not require agencies to follow the practices implicit in the model. We believe, however, that failure to do so can reduce the degree of assurance that appropriate security controls have been successfully incorporated into the system under development. The agencies' views are reflected in the report as appropriate.

Department of Commerce/ National Bureau of Standards

On January 21, 1988, the Department of Commerce provided written comments prepared by the National Bureau of Standards. The comments from the National Bureau of Standards were in two parts--managerial and technical (see app. III for the managerial comments). The National Bureau of Standards agreed with the general conclusion that more attention should be paid to security controls during the development process for automated information systems. NBS believed that the PCIE/NBS model developed over the past 4 years by the combined efforts of the President's Council on Integrity and Efficiency (which included GAO personnel) and NBS meets many of the concerns expressed in our draft report. We believe that the PCIE/NBS model is very similar in content to ours, in the areas that both address. Since the PCIE/NBS model is to be included in a forthcoming NBS Special Publication, we have decided to reference this model in our recommendations.

NBS states that guidance, such as OMB Circular A-130 and various Federal Information Processing Standards Publications, provide general, but quite clear guidance on security and control measures needed in automated systems. We disagree on the clarity and consistency of some of the federal guidance and provide examples of our concern in the report.

NBS, in its comments, recognizes its responsibilities under the Computer Security Act of 1987 to develop cost-effective standards and guidelines to protect the security and privacy of the sensitive information processed by the agencies and to develop validation and evaluation procedures for those standards and guidelines through research and liaison with other government and private agencies. NBS states that the activities prescribed in the act are necessary and appropriate and they are consistent with the Administration's goals of improving federal management operations. Further, it observes that this legislation could be a valuable aid to federal agencies in averting the problems addressed in our report. We concur.

We also address in the text of our report, as applicable, the technical comments and corrections offered by the National Bureau of Standards.

Office of Management and Budget

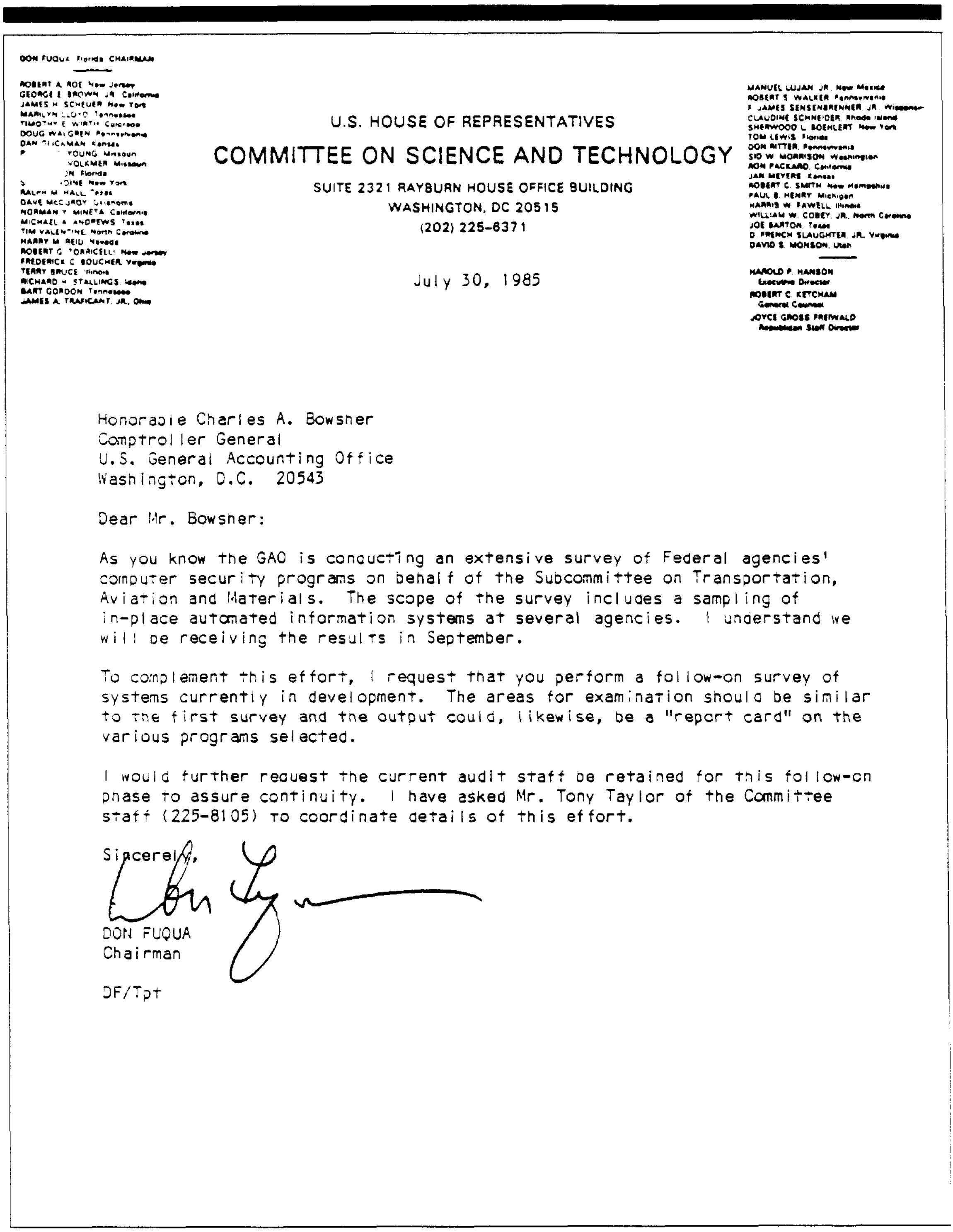
On January 20, 1988, OMB provided oral comments on a draft of this report. The Office agreed with the need to emphasize security in the development of information systems. OMB stated that the thrust of the security policy in Circular A-130 has been endorsed in the Computer Security Act of 1987. The OMB position is that the security requirements, including the security aspects of benefit/cost analyses, should be integrated into the overall information system benefit/cost analyses. OMB said that it will review its governmentwide information security policies to assure that they are consistent with the Computer Security Act of 1987.

OMB offered several specific comments on the draft report that were incorporated into this report as appropriate. The comments included a statement that OMB will continue to review the major Presidential Priority Systems and ensure that its reviews are consistent with the provisions of the Computer Security Act of 1987.

The General Services Administration

On January 21, 1988, the General Services Administration provided written comments on a draft of this report (see app. IV), including an update on its recent activities to improve security guidance in the FIRMR. We are concerned, however, that GSA did not discuss these activities in the context of the Computer Security Act of 1987, which requires (sec. 4., amendment to Brooks Act) that the Administrator shall revise the Federal Information Resources Management Regulation (41 CFR ch. 201) to be consistent with the standards and guidelines promulgated by the Secretary of Commerce (under sec. 4).

Request Letter



DON FUQUA Florida CHAIRMAN

ROBERT A. ROE New Jersey
GEORGE E. BROWN JR. California
JAMES H. SCHEUER New York
MARILYN LLOYD Tennessee
TIMOTHY E. WIRTH Colorado
DOUG WALGREN Pennsylvania
DAN GLICKMAN Kansas
P YOUNG Missouri
VOLKMER Missouri
ON Florida
S OINE New York
RALPH M. HALL Texas
DAVE McCURDY Oklahoma
NORMAN Y. MINETA California
MICHAEL A. ANDREWS Texas
TIM VALENTINE North Carolina
HARRY M. REID Nevada
ROBERT G. TORRICELLI New Jersey
FREDERICK C. BOUCHER Virginia
TERRY BRUCE Illinois
RICHARD H. STALLINGS Idaho
BART GORDON Tennessee
JAMES A. TRAFICANT, JR., Ohio

U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON SCIENCE AND TECHNOLOGY

SUITE 2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-6371

MANUEL LUJAN JR. New Mexico
ROBERT S. WALKER Pennsylvania
F. JAMES SENSENBRENNER, JR. Wisconsin
CLAUDINE SCHNEIDER Rhode Island
SHERWOOD L. BOEHLERT New York
TOM LEWIS Florida
DON RITTER Pennsylvania
SID W. MORRISON Washington
RON PACKARD California
JAN MEYERS Kansas
ROBERT C. SMITH New Hampshire
PAUL B. HENRY Michigan
HARRIS W. FAWELL Illinois
WILLIAM W. COBEY, JR., North Carolina
JOE BARTON Texas
D. FRENCH SLAUGHTER, JR., Virginia
DAVID S. MONSON, Utah

HAROLD P. HANSON
Executive Director
ROBERT C. KETCHAM
General Counsel
JOYCE GROSS FREIWALD
Republican Staff Director

July 30, 1985

Honorable Charles A. Bowsher
Comptroller General
U.S. General Accounting Office
Washington, D.C. 20543

Dear Mr. Bowsher:

As you know the GAO is conducting an extensive survey of Federal agencies' computer security programs on behalf of the Subcommittee on Transportation, Aviation and Materials. The scope of the survey includes a sampling of in-place automated information systems at several agencies. I understand we will be receiving the results in September.

To complement this effort, I request that you perform a follow-on survey of systems currently in development. The areas for examination should be similar to the first survey and the output could, likewise, be a "report card" on the various programs selected.

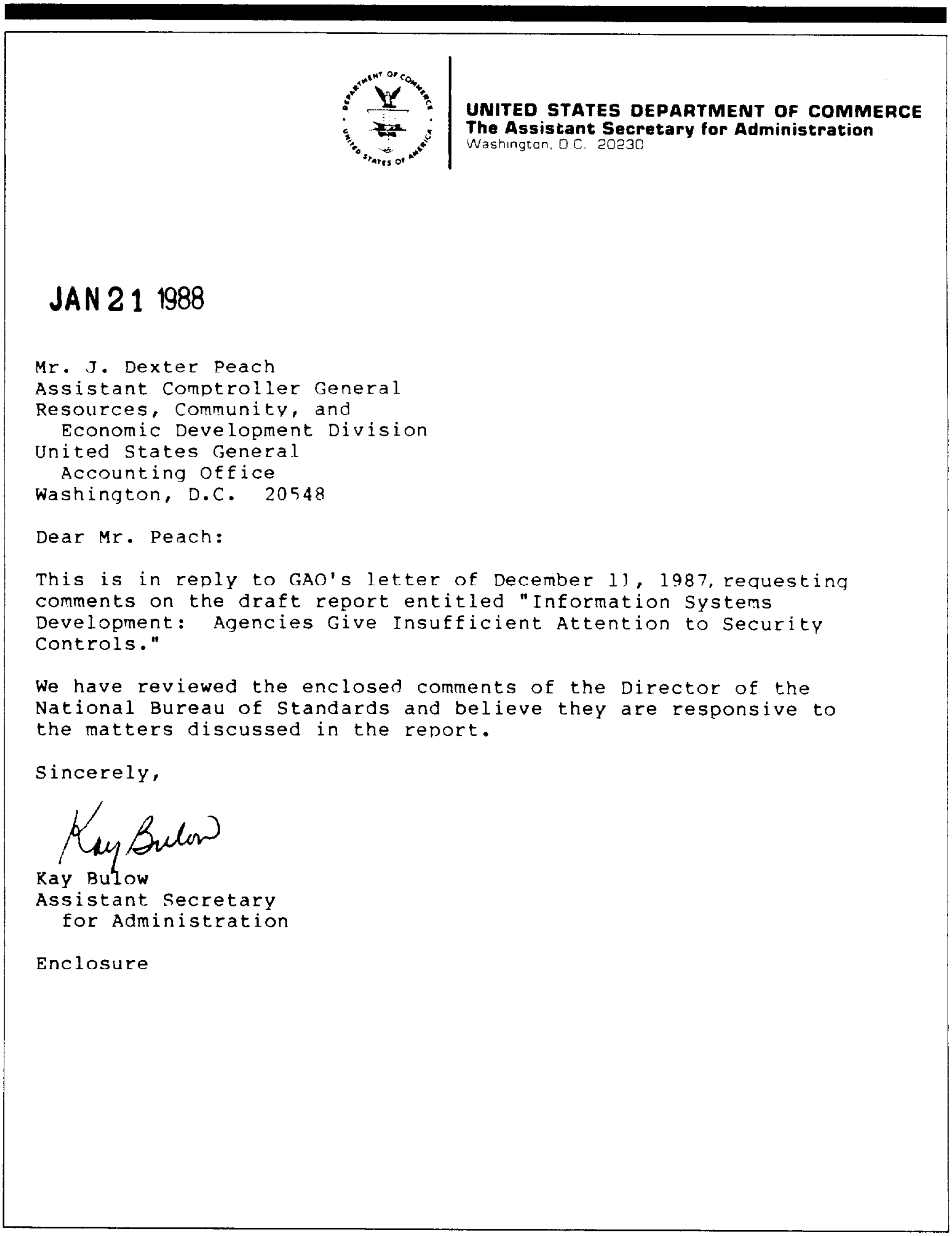
I would further request the current audit staff be retained for this follow-on phase to assure continuity. I have asked Mr. Tony Taylor of the Committee staff (225-8105) to coordinate details of this effort.

Sincerely,

DON FUQUA
Chairman

DF/Tpt

Comments From the Department of Commerce and National Bureau of Standards



UNITED STATES DEPARTMENT OF COMMERCE
The Assistant Secretary for Administration
Washington, D.C. 20230

JAN 21 1988

Mr. J. Dexter Peach
Assistant Comptroller General
Resources, Community, and
Economic Development Division
United States General
Accounting Office
Washington, D.C. 20548

Dear Mr. Peach:

This is in reply to GAO's letter of December 11, 1987, requesting comments on the draft report entitled "Information Systems Development: Agencies Give Insufficient Attention to Security Controls."

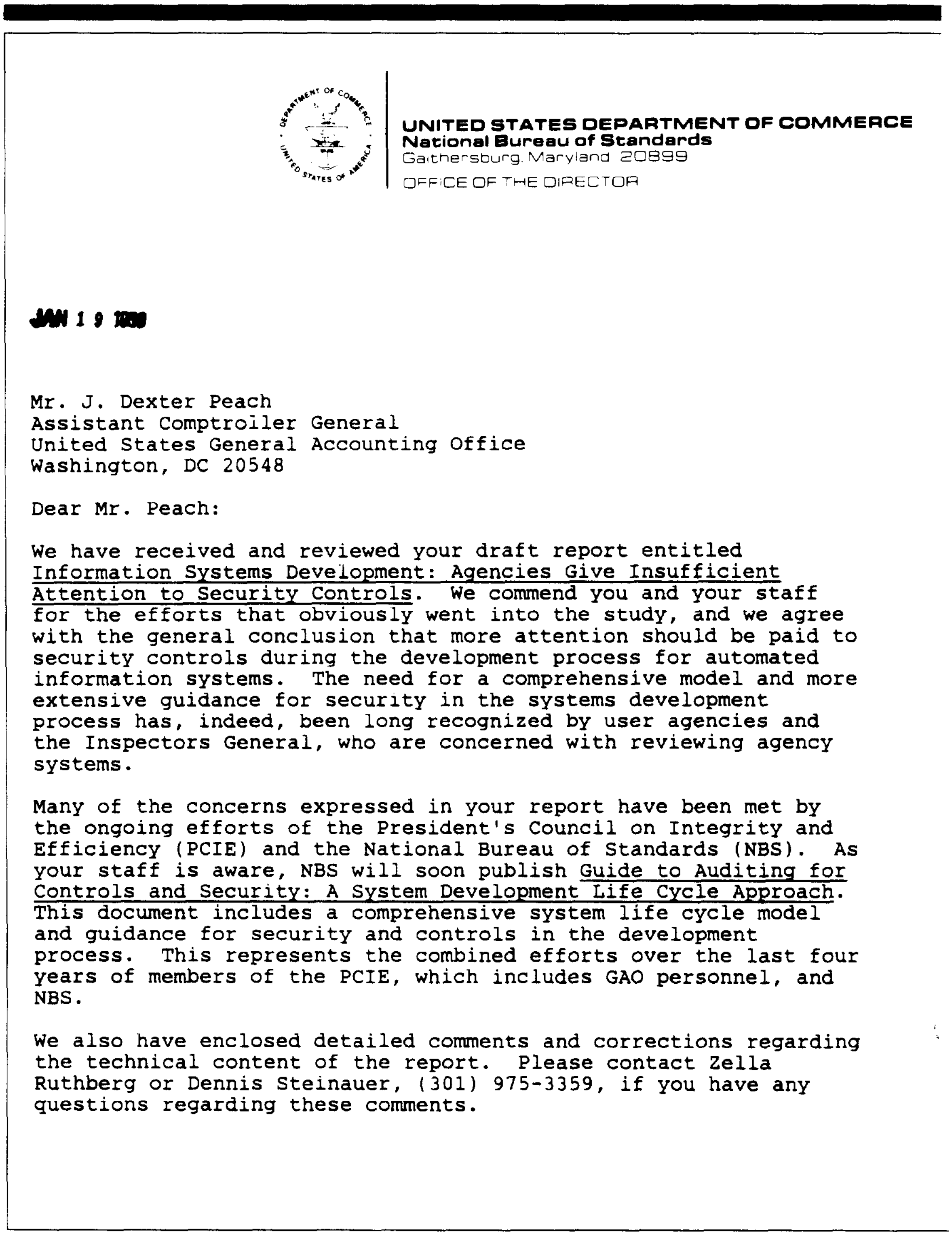
We have reviewed the enclosed comments of the Director of the National Bureau of Standards and believe they are responsive to the matters discussed in the report.

Sincerely,

Kay Bulow

Kay Bulow
Assistant Secretary
for Administration

Enclosure



UNITED STATES DEPARTMENT OF COMMERCE
National Bureau of Standards
Gaithersburg, Maryland 20899
OFFICE OF THE DIRECTOR

JAN 1 9 1988

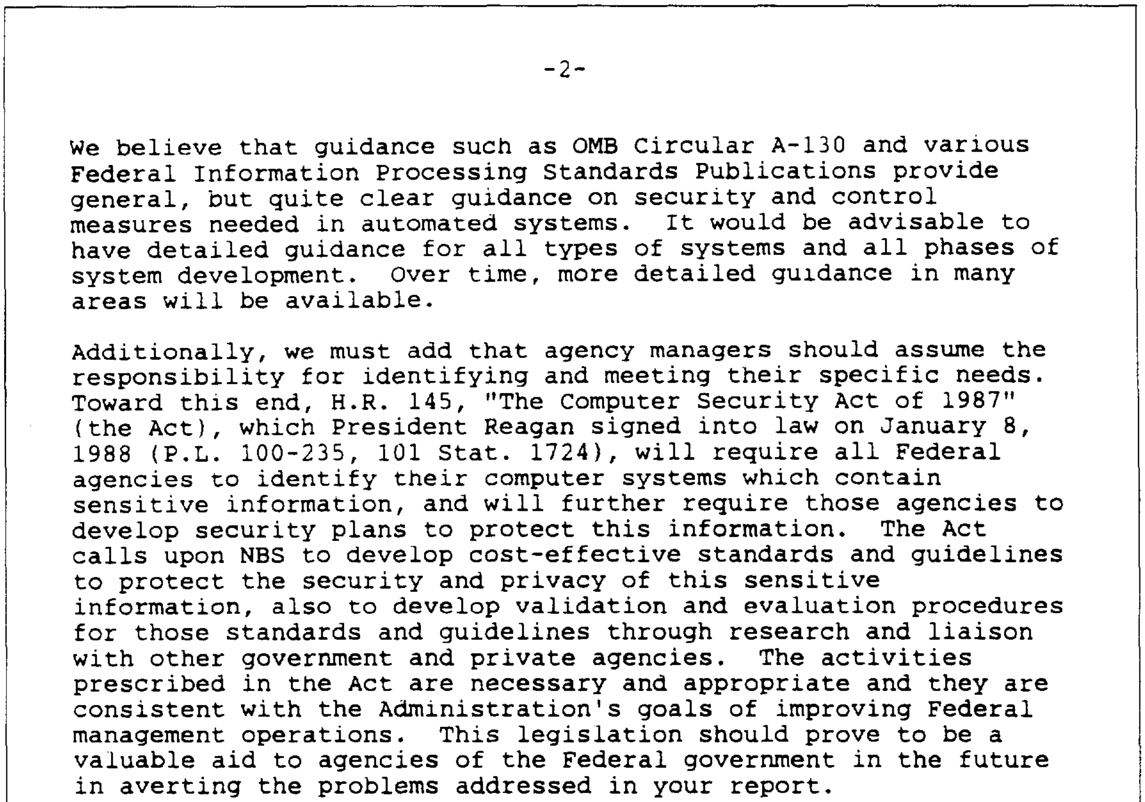
Mr. J. Dexter Peach
Assistant Comptroiler General
United States General Accounting Office
Washington, DC 20548

Dear Mr. Peach:

We have received and reviewed your draft report entitled Information Systems Development: Agencies Give Insufficient Attention to Security Controls. We commend you and your staff for the efforts that obviously went into the study, and we agree with the general conclusion that more attention should be paid to security controls during the development process for automated information systems. The need for a comprehensive model and more extensive guidance for security in the systems development process has, indeed, been long recognized by user agencies and the Inspectors General, who are concerned with reviewing agency systems.

Many of the concerns expressed in your report have been met by the ongoing efforts of the President's Council on Integrity and Efficiency (PCIE) and the National Bureau of Standards (NBS). As your staff is aware, NBS will soon publish Guide to Auditing for Controls and Security: A System Development Life Cycle Approach. This document includes a comprehensive system life cycle model and guidance for security and controls in the development process. This represents the combined efforts over the last four years of members of the PCIE, which includes GAO personnel, and NBS.

We also have enclosed detailed comments and corrections regarding the technical content of the report. Please contact Zella Ruthberg or Dennis Steinauer, (301) 975-3359, if you have any questions regarding these comments.



-2-

We believe that guidance such as OMB Circular A-130 and various Federal Information Processing Standards Publications provide general, but quite clear guidance on security and control measures needed in automated systems. It would be advisable to have detailed guidance for all types of systems and all phases of system development. Over time, more detailed guidance in many areas will be available.

Additionally, we must add that agency managers should assume the responsibility for identifying and meeting their specific needs. Toward this end, H.R. 145, "The Computer Security Act of 1987" (the Act), which President Reagan signed into law on January 8, 1988 (P.L. 100-235, 101 Stat. 1724), will require all Federal agencies to identify their computer systems which contain sensitive information, and will further require those agencies to develop security plans to protect this information. The Act calls upon NBS to develop cost-effective standards and guidelines to protect the security and privacy of this sensitive information, also to develop validation and evaluation procedures for those standards and guidelines through research and liaison with other government and private agencies. The activities prescribed in the Act are necessary and appropriate and they are consistent with the Administration's goals of improving Federal management operations. This legislation should prove to be a valuable aid to agencies of the Federal government in the future in averting the problems addressed in your report.

Thank you for the opportunity to comment on the report.

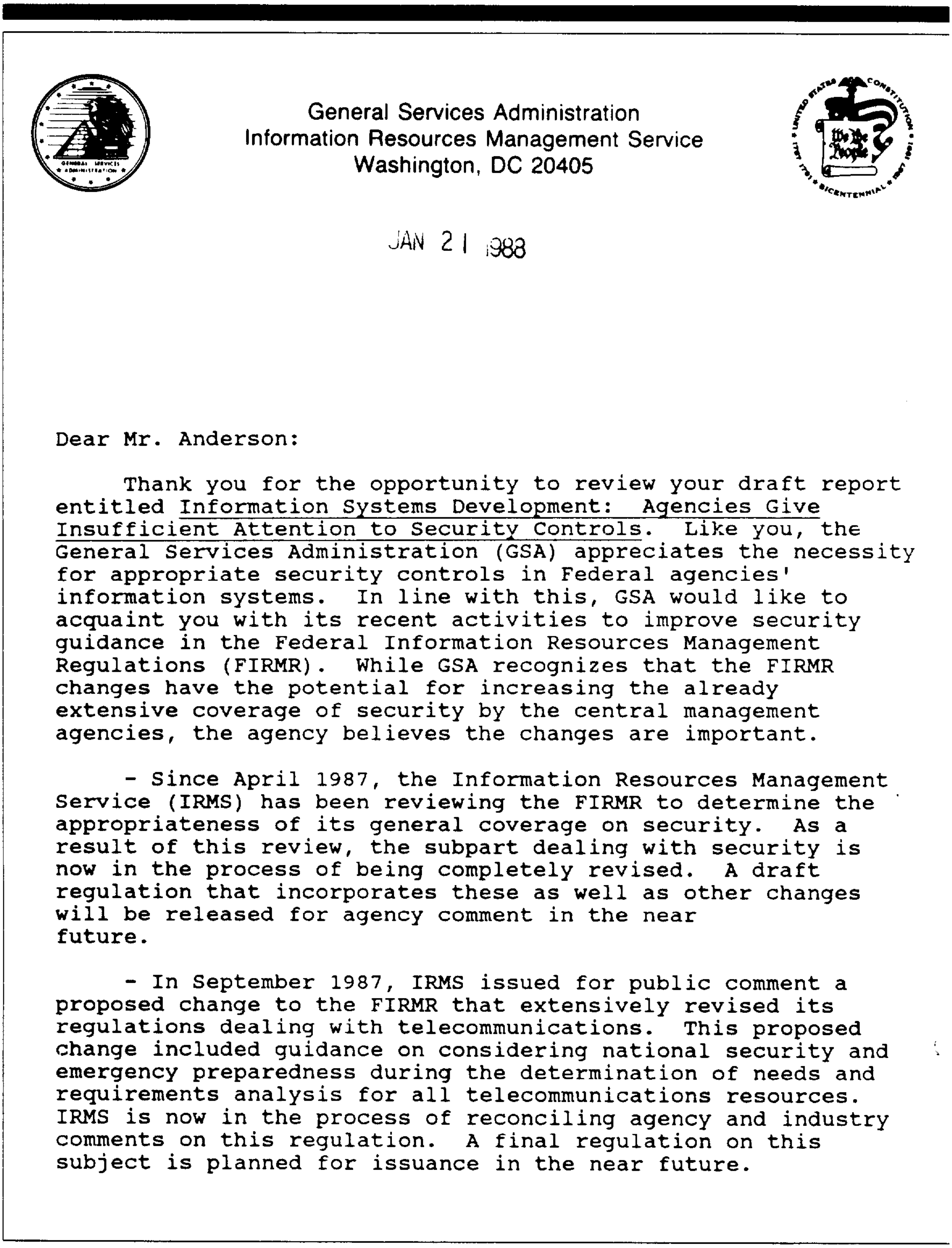
Sincerely,

E. Ambler.

Ernest Ambler
Director

Enclosure

Comments From the General Services Administration



General Services Administration
Information Resources Management Service
Washington, DC 20405

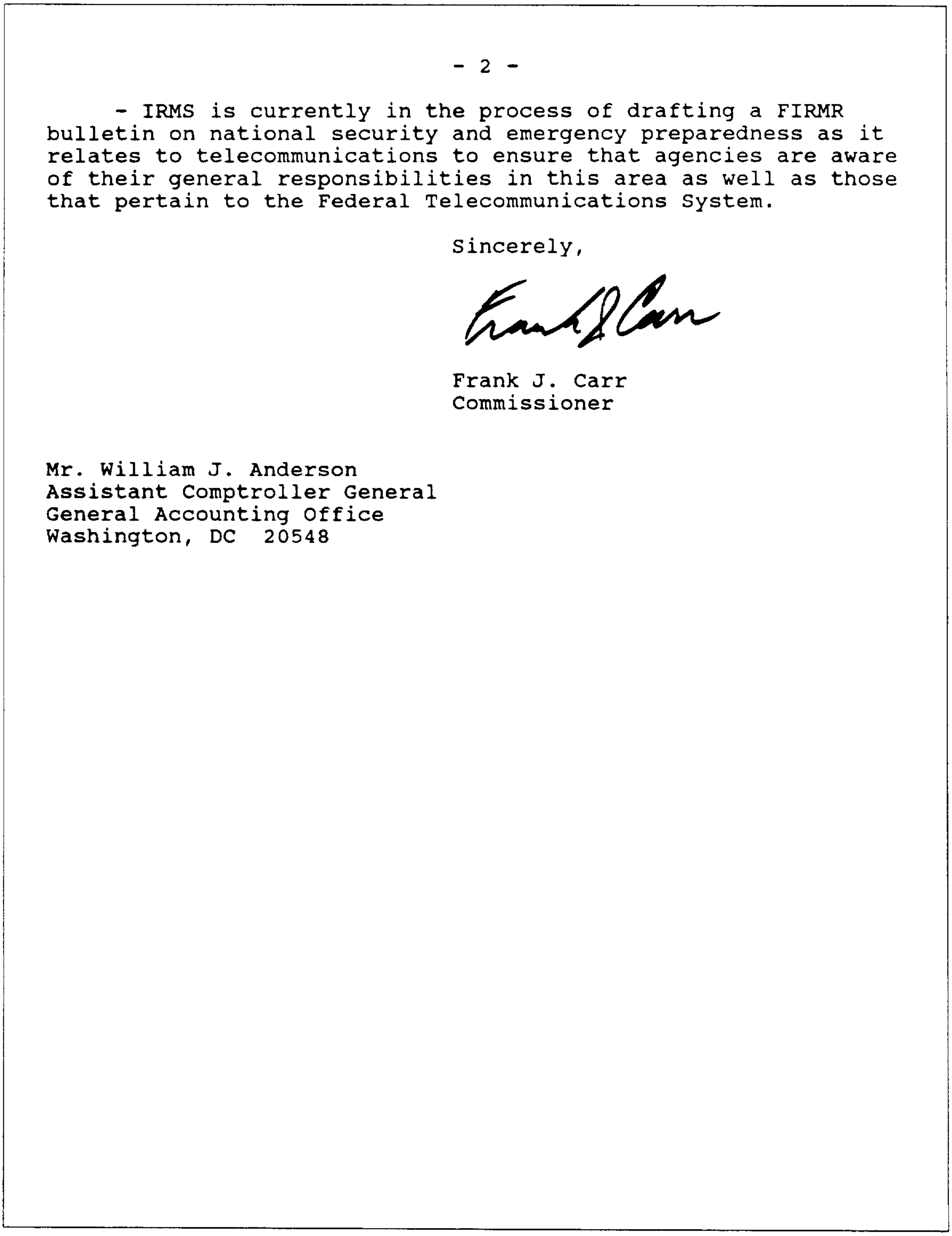
JAN 21 1988

Dear Mr. Anderson:

Thank you for the opportunity to review your draft report entitled Information Systems Development: Agencies Give Insufficient Attention to Security Controls. Like you, the General Services Administration (GSA) appreciates the necessity for appropriate security controls in Federal agencies' information systems. In line with this, GSA would like to acquaint you with its recent activities to improve security guidance in the Federal Information Resources Management Regulations (FIRMR). While GSA recognizes that the FIRMR changes have the potential for increasing the already extensive coverage of security by the central management agencies, the agency believes the changes are important.

- Since April 1987, the Information Resources Management Service (IRMS) has been reviewing the FIRMR to determine the appropriateness of its general coverage on security. As a result of this review, the subpart dealing with security is now in the process of being completely revised. A draft regulation that incorporates these as well as other changes will be released for agency comment in the near future.

- In September 1987, IRMS issued for public comment a proposed change to the FIRMR that extensively revised its regulations dealing with telecommunications. This proposed change included guidance on considering national security and emergency preparedness during the determination of needs and requirements analysis for all telecommunications resources. IRMS is now in the process of reconciling agency and industry comments on this regulation. A final regulation on this subject is planned for issuance in the near future.



- IRMS is currently in the process of drafting a FIRMR bulletin on national security and emergency preparedness as it relates to telecommunications to ensure that agencies are aware of their general responsibilities in this area as well as those that pertain to the Federal Telecommunications System.

Sincerely,

Frank J Carr

Frank J. Carr
Commissioner

Mr. William J. Anderson
Assistant Comptroller General
General Accounting Office
Washington, DC 20548

Glossary

Access

(1) A specific type of interaction between a subject (e.g., user or user process) and an object (e.g., 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 (e.g., user or user process) 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 (e.g., data).

Accreditation

The managerial authorization and approval, granted to an ADP system o 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-spec ified 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).

Availability

(1) The state that exists when required automated services can be obtained within an acceptable period. (2) The property which 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 co figuration item's life cycle. Baselines, plus approved changes from thos baselines, constitute the current configuration identification.

Certification

The technical evaluation of a system's security features, made as part 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.

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.

Compromise

A violation of the security system such that an unauthorized disclosure, modification, or destruction of sensitive information may have occurred or that a denial of service condition has been induced.

Computer Security

The protection of computers and their services from all natural and human-made hazards and 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.

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 i the source documents and have not been exposed to accidental or malicious alteration or destruction. (2) The property that data have not bee exposed to accidental or malicious alteration or destruction. (3) In a dat base system, avoidance of simultaneous update where two concurrentl executing transactions, each correct in itself, may interfere with each other so as to produce incorrect results.

Efficiency

The amount of computing resources and code required by a program to perform a function.

Environment

The aggregate of external circumstances, conditions, and objects that affect the development, operation, and maintenance of a system.

Information

Data that are communicated, interpreted, or processed.

Information Security

Generally considered to be the overall management, procedures, and controls necessary to assure accuracy, integrity, and continuity of oper ations for an information system.

Integrity

(1) For software quality, the extent to which access to software or dat by unauthorized persons can be controlled. (2) For computer, data bas and network security, see Data Integrity.

Journal

An audit trail of data base activities.

Network

A network is composed of a communications medium and all components attached to that medium whose responsibility is the transferenc of information. Such components may include, but are not limited to, hosts, packet switches, telecommunications controllers, key distributic centers, access control centers, technical control devices, and other cor ponents used by the network. Network delimitation is best expressed i terms of the protocol layers.

Password

A private character string that is used to authenticate an identity.

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.

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 CPU time, terminal connect time, amount of directly-addressable memory, disk space, number of input/output requests per minute.

Risk Analysis

An analysis of system assets and vulnerabilities to establish an expected annual loss (EAL) 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 which 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 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 Verification.

Sensitive Information

Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act (U.S.C. Title 5, sec. 552a), 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.

User

(1) Any person who interacts directly with a computer system. This includes both those persons who are authorized to interact with the system and those people who interact without authorization (e.g. active or passive wiretappers). 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.

*U.S. G.P.O. 1988-201-749:80136

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.