DOCUMENT RESUME

ED 223 255 IR 050 012

TITLE	Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices.
INSTITUTION	General Accounting Office, Washington, D.C.
REPORT NO	MASAD-82-18
PUB DATE	21 Apr 82
NOTE	42p.
AVAILABLE FROM	U.S. General Accounting Office, Document Handling and Information Services Facility, PO Box 6015, Gaithersburg, MD 20760 (first five copies, free).
PUB TYPE	Viewpoints (120) -- Reports - Evaluative/Feasibility (142)
EDRS PRICE	MF01/PC02 Plus Postage.
DESCRIPTORS	Automation; *Computers; *Confidentiality; *Federal Government; Federal Regulation; Information Networks; *Information Systems; Public Administration; Public Agencies; *Telecommunications
IDENTIFIERS	*Computer Security; General Services Administration; National Bureau of Standards; Office of Management and Budget; Office of Personnel Management

ABSTRACT

This evaluation of information security programs in the executive agencies of the U.S. federal government was requested by the Subcommittee on Government Information and Individual Rights, a part of the Congressional Committee on Government Operations. The report focuses on automated systems for personal, proprietary, and other sensitive information, particularly systems using telecommunication networks. Evaluation results indicate that a reasonable level of protection over information systems is not being provided. Accordingly, 10 recommendations for improvement are made. A glossary of terms precedes the five appendices which constitute the largest part of the report. These appendices comprise: (1) a review of the study's objectives, scope, and methodology; (2) a discussion of the automated information security problem; (3) an examination of four reasons why Office of Management and Budget (OMB) security guidelines do not provide sufficiently comprehensive policy and guidance to executive agencies; (4) an explanation of why central executive agencies are not effective in fulfilling their information security program responsibilities; and (5) a demonstration of the fact that senior agency management gives only limited support to automated information security programs. A diagram of telecommunication network vulnerabilities and a map illustrating the telecommunication networks of three civil federal agencies are provided. (ESR)

FEDERAL INFORMATION SYSTEMS REMAIN HIGHLY VULNERABLE TO FRAUDULENT, WASTEFUL, ABUSIVE AND ILLEGAL PRACTICES

Report by the U.S. Federal Accounting Office

MASAD 82-18
April 21, 1982

UNITED STATES GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

MISSION ANALYSIS AND
SYSTEMS ACQUISITION DIVISION

B-198551

The Honorable Glenn English
Chairman, Subcommittee on Government
Information and Individual Rights
Committee on Government Operations
House of Representatives

Dear Mr. Chairman:

The former chairman requested we undertake an evaluation of the information security programs in the executive agencies. He was concerned that these programs were currently receiving less attention from senior management than they had in the past.

Specifically, he wanted to know:

--Whether Office of Management and Budget (OMB) Circular A-71, Transmittal Memorandum No. 1 (July 27, 1978), "Security of Federal Automated Information Systems," contained appropriate policy and guidance to provide a reasonable (acceptable) level of protection over information systems if fully implemented by the executive agencies.

--How effective the central agencies are in fulfilling their Government-wide information security program responsibilities. The central agencies include OMB, Department of Commerce, General Services Administration (GSA), and the Office of Personnel Management (OPM).

--What the executive agencies are doing to implement Government-wide information security program policy and guidance.

--What, if anything, the executive agencies must do to achieve a reasonable level of protection over their automated information systems, particularly those using telecommunication networks.

The former chairman's concern was based on the executive agencies' lack of any substantive efforts to improve the level

of protection provided over their automated information systems following our January 1979 report. 1/

In April 1980 we provided the former chairman an interim report 2/ that focused on how effective the central agencies were in fulfilling their Government-wide information security program responsibilities. In essence, this interim report showed that the central agencies were not effective because they have given only limited support to the program. Also, several of our previous reports showed that the Government's information systems are highly vulnerable to fraudulent, wasteful, abusive, and illegal practices.

The purpose of this report is to address all the issues raised in the former chairman's December 1979 request and to place those issues and the ones described in our January 1979 and April 1980 reports into perspective so that the reasons why automated information systems in the executive agencies remain highly vulnerable to abusive and unauthorized practices can be more easily understood and corrected.

The conditions disclosed during our current evaluation demonstrate that little change or improvement has occurred since our prior evaluations. During our current evaluation we found that:

--OMB Circular A-71, Transmittal Memorandum No. 1, is not sufficiently comprehensive to provide needed policy and guidance to executive agencies for establishing a reasonable level of protection over their automated information systems. (See app. III.)

--The central agencies have not been effective in fulfilling their automated information security program responsibilities. (See app. IV.)

--Executive agencies are doing little to implement information security program policy and guidance. (See app. V.)

--Executive agencies have not developed and maintained a total system of controls to eliminate the fraudulent, wasteful, abusive, and illegal practices to which their automated

---

1/"Automated Systems Security--Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data" (LCD-78-123, Jan. 23, 1979). Also, see our March 21, 1979, report (LCD-79-109) to the Secretary of Defense which supplements the January 1979 report.

2/"Central Agencies Compliance With OMB Circular A-71, Transmittal Memorandum No. 1" (LCD-80-56-I, Apr. 30, 1980).

information systems have been and are being subjected. (See app. II.)

Collectively, these conditions have precluded the establishment and maintenance of a reasonable level of protection over automated information systems used by executive agencies, but more specifically:

--The deficiencies in OMB Circular A-71, Transmittal Memorandum No. 1, must be removed because they have left some executive agencies confused as to the nature and extent to which the memorandum is to be implemented and its application to technologically complex automated information systems, particularly those using telecommunication networks.

--The ineffective information security programs of the central agencies have been a primary contributing factor to the continued vulnerability of the automated information systems in the executive agencies. In particular, OMB must take the lead, along with other central agencies, in ensuring that information security and related standards and guidelines are effectively implemented Government-wide.

--The increasing Federal investments in automated information systems result in increased vulnerabilities for fraudulent, wasteful, abusive, and illegal practices because greater concentrations of information are accessible from remote terminals. Because limited support from senior management in the executive agencies has resulted in their information systems becoming even more vulnerable to abusive and unauthorized practices, requirements for corrective action plans must be imposed on senior management as must accountability for their implementation.

Accordingly, we recommend that the Director of OMB:

--Revise OMB Circular A-71, Transmittal Memorandum No. 1, to (1) identify the minimum controls necessary for ensuring a reasonable level of protection over personal, proprietary, and other sensitive information, (2) clarify the interrelationship between Transmittal Memorandum No. 1 and policy and guidance on safeguarding information classified for purposes of national security, (3) clarify when executive agencies must afford the same level of protection against unauthorized disclosure of personal, proprietary, and other sensitive information as they do to information classified for purposes of national security, and (4) establish policy and specific guidance for achieving a reasonable level of protection over those systems, using telecommunication networks.

--Require executive agencies to submit to OMB, for review and approval, new plans for establishing and maintaining a

reasonable level of protection over their automated information systems, in accordance with a revised Transmittal Memorandum No. 1, as recommended on page 3. This includes establishing and maintaining an effective internal evaluation of their automated information security programs.

--Develop procedures for ensuring executive agencies' implementation of their automated information security program plans. Implementation of these plans should be integrated into the budget process so that major automated information systems are designed, developed, operated, and maintained with a reasonable level of protection. Each system should have a restricted statement of the potential vulnerabilities, the specific security program to be used, and the expected level of risk when the security program is implemented; that is, what vulnerabilities will exist even with the implementation of the security program.

--Fully implement other OMB responsibilities as specified in the Paperwork Reduction Act of 1980 and as they relate to information security programs involving Federal automated data processing systems and telecommunication networks. Specifically, the Director of OMB should:

  --Provide advice and guidance on the acquisition and use of automated data processing and telecommunications equipment, and coordinate through the review of budget proposals and other methods, agency proposals for acquisition and use of such equipment. Implementation of this responsibility combined with a review of agencies' plans for establishing and maintaining a reasonable level of protection over their automated information systems will help ensure implementation of such plans.

  --Monitor the effectiveness of, and agencies' compliance with, Public Laws 87-847 (Federal Telecommunications Fund) and 89-306 (often called the Brocks Act).

  --Initiate and review proposals for changes in legislation, regulations, and agency procedures to improve automated data processing and telecommunications practices to ensure a reasonable level of protection over personal, proprietary, and other sensitive information as developed and maintained by the executive agencies.

  --Through a review of budget proposals, inform the President and the Congress of the progress made to develop and maintain a reasonable level of protection over personal, proprietary, and other sensitive information in the executive agencies.

The central agencies must work together more cooperatively to coordinate policies, principles, standards, and guidelines

for information protection to substantially reduce the vulnerabilities and risks presently associated with executive agencies' automated information systems. Specifically, we recommend

--the Directors of OMB, the National Bureau of Standards (NBS), and OPM collaborate with the Administrator of GSA to completely cross-reference their information security standards and guidelines in the Federal Property Management Regulations and

--the Administrator of GSA completely cross-reference OMB, NBS, and OPM information security policies, principles, standards, and guidelines in the Federal Property Management Regulations to eliminate the confusion that presently exists with their use.

We further recommend that the heads of executive departments and agencies

--identify, in accordance with a revised Transmittal Memorandum No. 1, the vulnerabilities and risks associated with their automated information systems and develop a new plan for establishing a reasonable level of protection over those systems;

--identify a time schedule and resource requirements for implementing the plan;

--establish internal review audit programs which will periodically evaluate and report on the level of protection actually provided over automated information systems; and

--include with their next budget request a report describing the actions taken to implement the plan and to implement recommendations made by the agency internal review group.

A more detailed description of the objectives, scope, and methodology used in making this evaluation is contained in appendix I.

Agency comments were not requested from the central and executive agencies according to a request received from your office.

Also, as requested by your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days from the date of the report. At that time, we will send copies to interested parties and make copies available to others upon request.

Sincerely yours,

W. H. Shelley, Jr.
Director

Contents

ABBREVIATIONS

DOD	Department of Defense
GSA	General Services Administration
NBS	National Bureau of Standards
NCSC	National Communications Security Committee
OMB	Office of Management and Budget
OPM	Office of Personnel Management

GLOSSARY

Administrative controls	Administrative controls involve the management constraints, operational procedures, accountability procedures, and supplemental controls established to provide an acceptable level of protection for information. (For more details see Federal Information Processing Standards Publication No. 39, Glossary for Computer Systems Security, February 1976 and Security of Federal Automated Data Processing and Telecommunications, Federal Property Management Regulations, Subpart 101-35.3 (Amendment F-42, Aug. 1980)).
Automated information system	An automated information system is one which uses a computer to process and store information.
Information security	Information security is the protection necessary to safeguard personal and other sensitive information processed or stored in a computer system or transmitted and received through a telecommunication network. It is subject to violation at any point from information origination to the final disposition or destruction of the information. To minimize or prevent such violations and the consequences associated with them requires the combined use of three general types of controls--administrative, physical, and technical. Thus, information security requires that a total systems perspective be used to achieve a reasonable level of protection over personal and other sensitive data. (For more details, see Federal Property Management Regulation, Subpart 101-35.3.)
Physical controls	Physical controls include those described in Federal Information Processing Standards Publication No. 31; Federal Property Management Regulations; Guidelines for Automatic Data Processing; Physical Security and Risk Management, Subpart 101-36.7; and Environment and Physical Security, Subpart 101-35.3. These controls involve those used in the computer room, data control and conversion area, data file storage area, programmer's

	area, forms storage area, and the mechanical equipment room. These controls are intended to provide physical protection and access control to these areas to prevent damage or loss of information and equipment due to theft, vandalism, sabotage, espionage, civil disorder, and other forced intrusions.
Reasonable (acceptable) level of protection	A reasonable (acceptable) level of protection is a level of protection that allows authorized individuals to obtain access to and use only that information for which they have a valid requirement and only for valid or authorized purposes.
Technical controls	Technical controls include those incorporated into the equipment and software to prevent or minimize unauthorized penetration of the information system for unauthorized or illegal purposes. Physical and administrative controls involve areas other than the equipment and software. Technical controls, however, deal solely with the equipment and related software. This is the reason a reasonable level of protection can be achieved only through the combined use of all three types of controls. (For more details see Federal Property Management Regulations Subpart 101-35.3.)
Telecommunication networks	A telecommunication network provides access to a computer through the combined use of remote terminals and communications lines.

APPENDIX I

OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

The former chairman, Subcommittee on Government Information and Individual Rights, Committee on Government Operations, House of Representatives, requested we determine:

--Whether OMB Circular A-71, Transmittal Memorandum No. 1 (July 27, 1978), "Security of Federal Automated Information Systems," contained appropriate policy and guidance to provide a reasonable (acceptable) level of protection over information systems if fully implemented by the executive agencies.

--The effectiveness of the central agencies in fulfilling their Government-wide information security program responsibilities. The central agencies include OMB, Department of Commerce, GSA, and OPM.

--What the executive agencies are doing to implement Government-wide information security program policy and guidance.

--What, if anything, the executive agencies must do to achieve a reasonable level of protection over their automated information systems, particularly those using telecommunication networks.

SCOPE

Our evaluation was performed primarily from March to December 1980. From December 1980 through November 1981 we updated and supplemented our initial evaluation to include work accomplished on automated information security programs by the Office of the Secretary of Defense, the National Security Agency, and the National Communications Security Committee (NCSC).

Our evaluation concentrated on executive agencies' automated information security programs for personal, proprietary, and other sensitive information. We evaluated the administrative, physical, and technical controls used by selected executive agencies to provide protection over personal, proprietary, and other sensitive information. Our evaluation generally excluded information classified for purposes of national security because executive orders, National Communication Security directives, and laws such as the Atomic Energy Act of 1954 govern the manner in which security must be provided over this type of information. The major exception to this exclusion was where personal, proprietary, and other sensitive information was processed at agencies which deal solely or predominantly with information classified for purposes of national security.

We performed our evaluation at major executive agencies which included the Departments of Commerce, Defense, Education, Energy, Health and Human Services, and Treasury. We also performed our evaluation at the Internal Revenue Service and reviewed guidance available from OMB, NBS, GSA, and OPM.

METHODOLOGY

We examined pertinent documents and conducted in-depth interviews with key agency officials to obtain information on current and planned automated information security efforts.

We discussed with senior level executive agency officials the usefulness of Government-wide policies, principles, standards, and guidelines intended to be used in developing agency information security programs and the officials' level of involvement with the programs. We asked questions of operational level officials and reviewed pertinent documents concerning proposed and existing agency procedures for providing a reasonable level of protection for their automated information systems.

We evaluated pertinent developments in automated security as underway at DOD and NBS. For example, we discussed the Computer Security Evaluation Center 1/ established by DOD and a draft NBS publication on auditing computer security. Further, we reviewed NCSC reports on information security in the executive agencies. Although we did not have the resources to validate the extensive efforts of NCSC, we compared their conclusions and recommendations with independent efforts of the Office of the Secretary of Defense that resulted in the establishment of a DOD Computer Security Evaluation Center. This center was approved by the Deputy Secretary of Defense, effective January 1, 1981, and is operated by the National Security Agency.

Our evaluation was performed in accordance with our "Standards for Audit of Governmental Organizations, Programs, Activities, and Functions."

1/Currently the DOD Computer Security Center.

THE AUTOMATED INFORMATION SECURITY PROBLEM

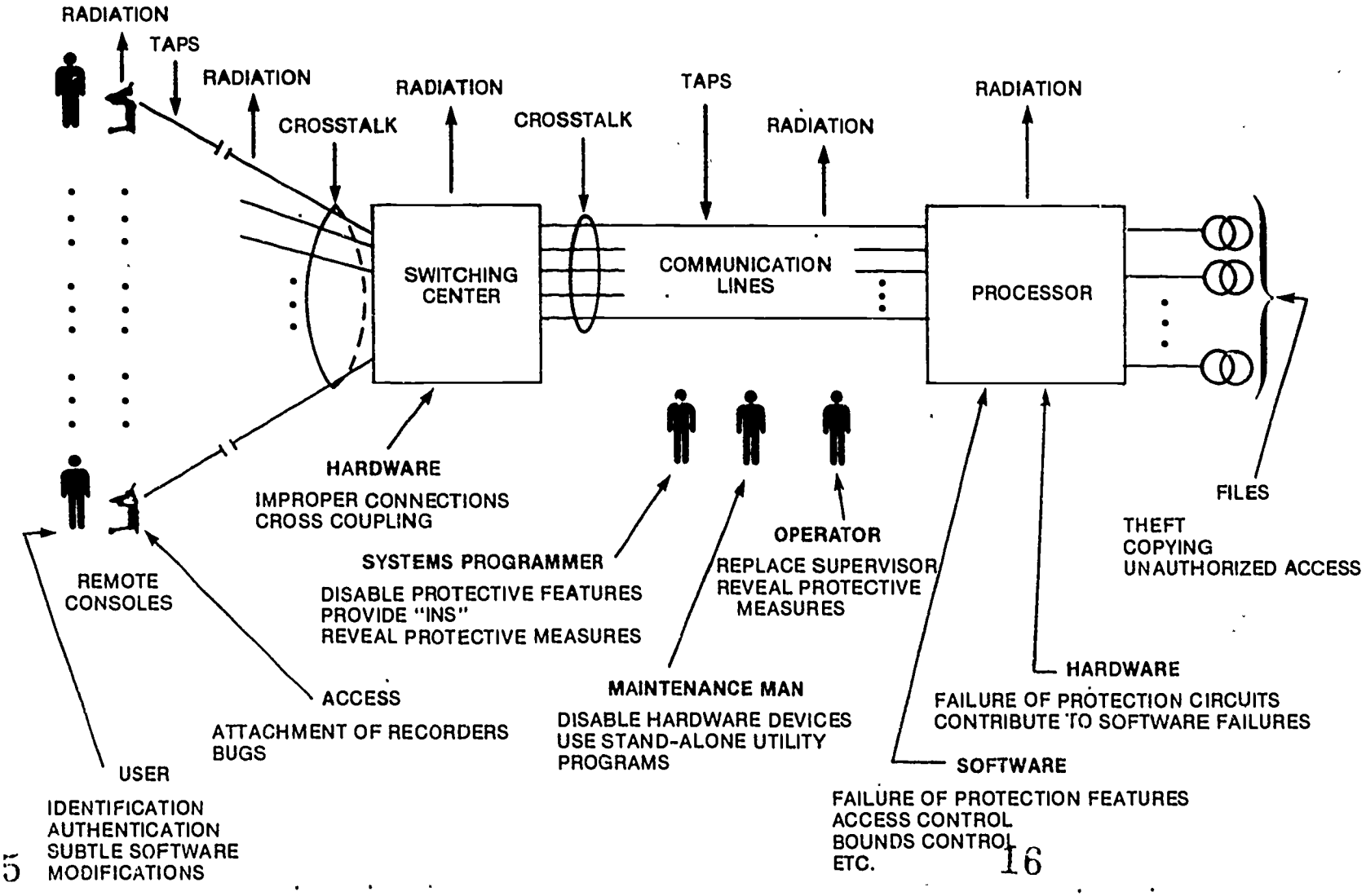
This appendix demonstrates that automated information systems in the executive agencies are highly vulnerable to fraudulent, wasteful, abusive, and illegal practices, and describes why there is a growing need to provide a reasonable level of protection over such systems, particularly those using telecommunication networks. This information is intended to place into perspective issues contained in our previous reports and in this report so that the reasons for the problem can be more easily understood and corrected.

NATURE OF THE INFORMATION SECURITY PROBLEM

Information security must be approached from a total systems perspective. An information system is comprised of several functions, such as data origination, recording, transmission for processing, processing, storage, retrieval, dissemination, use, and destruction. Each function requires a separate set of administrative, physical, and technical controls which collectively must operate as a total system of controls to achieve a reasonable and cost-effective level of protection over the data. The design, development, implementation, and maintenance of a total system of controls is a complex and comprehensive problem, particularly when a telecommunication network is used to gain access to and to retrieve information from a computer. The complexity of providing a total system of controls when using a telecommunication network is attributable to the diverse variety of equipment (hardware), people, and software needed to provide the required capability and the organizational and technological environment in which these components must operate.

As shown in Figure 1 on page 4, natural failures of equipment and software or improper connections can result in the computer being used for unauthorized purposes. However, we believe that users, programmers, computer operators, and even maintenance personnel pose a much more serious threat to the integrity of information security than do natural failures of either the hardware or the software. For example, users have been known to tape on to or over computer terminals system log-in/log-off procedures and their individual access identifiers. This condition allows unauthorized users to readily gain access to, manipulate, and retrieve information by masquerading as valid or authorized users. Programmers and computer operators may be able to make unauthorized changes or alterations to software while information is being processed or use the computer for unauthorized or illegal purposes. Maintenance personnel may make unauthorized copies of data files which are then used for illegal purposes. The organizational and technological environment also contributes to these conditions because of the lack of a total system of controls which can minimize these occurrences. These conditions will increase and become more complex as executive agencies make greater use of telecommunication networks.

FIGURE 1 TELECOMMUNICATION NETWORK VULNERABILITIES



APPENDIX II

APPENDIX II

IMPACT OF TELECOMMUNICATION NETWORKS

Figure 2 on page 6 shows the geographical coverage of only three dedicated telecommunication networks used by executive agencies and illustrates the variety and complexity of the transmission paths and facilities. While this map is limited to networks used by only three agencies, we are aware of at least 31 such dedicated telecommunication networks used throughout the Federal Government. These networks have wide geographic coverage and are listed below:

Department/agency	Number of major networks
Agriculture	4
Commerce	7
Energy	2
Health and Human Services	4
Interior	2
Justice	7
Treasury	4
Veterans Administration	1
Total	31

The use of telecommunication networks supports executive agency computer use. These networks were not established in a coordinated, cost effective, and secure manner. The fiscal year 1983 budget request illustrates that there will be a significant growth in executive agencies' use of telecommunication networks.

In our 1976 report we showed that automated information systems were susceptible to criminal activities. 1/ In another report 2/ we showed that Federal systems were quite vulnerable to fire, flood, sabotage, and theft or misuse. In 1977 3/ we showed that the Government's telecommunication systems were exceedingly vulnerable to various penetration techniques for gaining access to the system and to intercepting information carried over the system. That report also showed that unauthorized information could be easily inserted into the system for fraudulent purposes.

Other reports showed that the Internal Revenue Service needed to improve its security program to protect the confidentiality of

---

1/"Computer-Related Crimes in Federal Programs" (FGMSD-76-27, Apr. 27, 1976).

2/"Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities" (FGMSD-76-40, May 10, 1976).

3/"Vulnerabilities of Telecommunications Systems to Unauthorized Use" (LCD-77-102, Mar. 31, 1977).

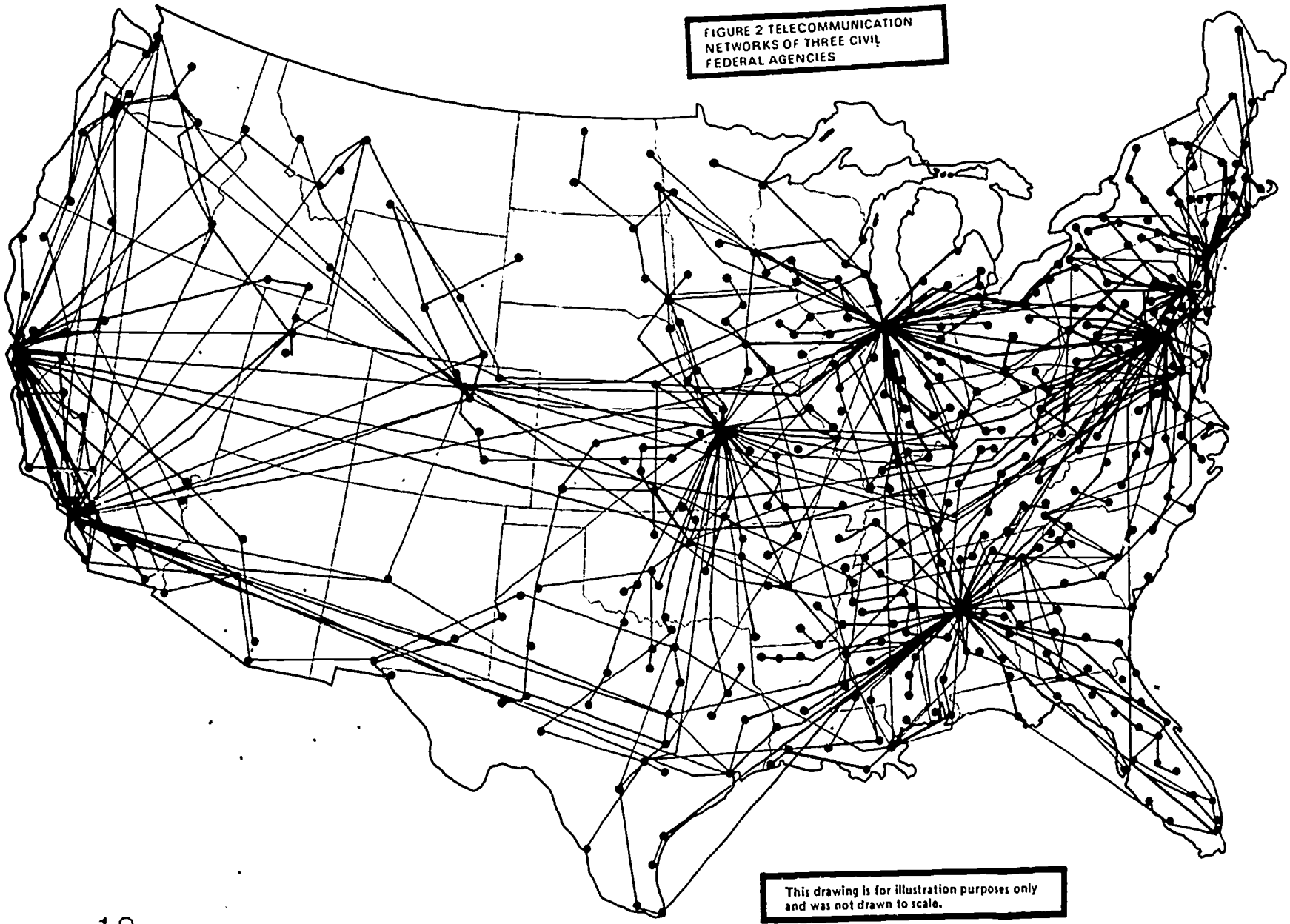


FIGURE 2 TELECOMMUNICATION NETWORKS OF THREE CIVIL FEDERAL AGENCIES

This drawing is for illustration purposes only and was not drawn to scale.

income tax information, 1/ flaws in the controls in the systems used by the Social Security Administration caused millions of dollars in erroneous payments, 2/ and computer security weaknesses in the Community Services Administration helped to make the system exceedingly vulnerable to fraud and abuse. 3/

More recently 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 another instance, Internal Revenue Service 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 perform outside consulting work, to gain access to and use proprietary data, and to make unauthorized and premature disclosure of information considered by Agriculture to be highly sensitive.

INCREASED VULNERABILITY OCCURS AS INVESTMENT RISES IN AUTOMATED INFORMATION SYSTEMS

As illustrated, executive agencies' automated information systems and the assets they control are exceedingly vulnerable to misuse, abuse, and theft. As these agencies expand their use of telecommunication networks, their information systems will become even more vulnerable to these improper or illegal activities unless senior management devotes more attention and resources to establishing a reasonable level of protection over those systems.

The increased vulnerability occurs because of the increased concentration of sensitive information in electronic form. Large amounts of sensitive information, such as income tax data, are susceptible to user error, hardware/software error, and deliberate attack.

1/"IRS' Security Program Requires Improvements to Protect Confidentiality of Income Tax Information" (GGD-77-44, July 11, 1977).

2/"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).

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

More comprehensive controls become necessary because growing numbers of remote computer terminals may provide access to very large data bases. Without adequate controls, errors or deliberate attacks are difficult to discover under these circumstances. Also, it may be very difficult to discover and fix errors in a large data base.

ISSUES ASSOCIATED WITH THE AUTOMATED INFORMATION SECURITY PROGRAMS ARE COMPLEX AND INTERRELATED

There are several factors which must be addressed to provide a reasonable level of protection over executive agencies' automated information system programs. The examples we previously cited of fraudulent, wasteful, abusive, and illegal practices to which these systems have been subjected demonstrate how vulnerable these systems are. The following appendixes describe in more detail factors that must be addressed to provide a reasonable level of protection for automated information systems in executive agencies. These factors can be summarized as follows.

--Existing information security program policy and guidance must be clear and explicit. (See app. III.)

--The central agencies have a major role in giving the right kind of support and direction to the executive agencies. (See app. IV.)

--The executive agencies have the major burden of ensuring that implementation of a reasonable level of protection over their automated information systems is accomplished. (See app. V.)

APPENDIX III

OMB CIRCULAR A-71, TRANSMITTAL MEMORANDUM NO. 1, IS NOT SUFFICIENTLY COMPREHENSIVE TO PROVIDE NEEDED POLICY AND GUIDANCE TO EXECUTIVE AGENCIES

OMB Circular A-71, Transmittal Memorandum No. 1, is not sufficiently comprehensive to provide needed policy and guidance to executive agencies for establishing a reasonable level of protection over their automated information systems. Specifically, the memorandum does not (1) identify the minimum controls necessary for ensuring a reasonable level of protection over personal, proprietary, and other sensitive information, (2) clarify the relationship between Transmittal Memorandum No. 1 and policy and guidance on safeguarding information classified for purposes of national security, (3) clarify when executive agencies must afford the same level of protection against unauthorized disclosure of personal, proprietary, and other sensitive information as they do to information classified for purposes of national security, and (4) establish policy and specific guidance for achieving a reasonable level of protection over those systems using telecommunication networks. These deficiencies have contributed to the limited support senior management in the executive agencies has given to their automated information security programs.

All information that is originated, collected, transmitted for processing, processed, stored, retrieved, disseminated, used, and destroyed by executive agencies is subject to being misused for fraudulent, wasteful, abusive, and illegal purposes. A total system of controls is needed to minimize the use of information for such purposes. The extent to which these controls are necessary depends on whether the information is (1) classified for purposes of national security or (2) considered to be personal, proprietary, or sensitive for other reasons. A much more sophisticated system of controls is needed to protect information classified for purposes of national security than is required to protect personal, proprietary, or other sensitive information. Government-wide policy used by executive agencies as a basis for establishing and maintaining a reasonable level of protection over their information systems should be comprehensive enough to provide the needed guidance. OMB Circular A-71, Transmittal Memorandum No. 1, does not meet this goal.

SENSITIVE INFORMATION

Transmittal Memorandum No. 1 makes the head of each executive agency responsible for ensuring a reasonable level of security for all agency information whether processed in-house or commercially. Each executive agency head is responsible for ensuring security of all agency information, including the responsibility for the establishment of administrative, physical, and technical safeguards required to adequately protect personal, proprietary, or other sensitive information not subject to national security regulations. The memorandum defines "sensitive data" (information) as follows:

> "Sensitive data is data which requires a degree of protection due to the risks and magnitude of loss or harm which could result from inadvertent or deliberate disclosure, alteration, or distribution of the data (e.g., personal data, proprietary data)."

While Transmittal Memorandum No. 1 requires the head of each executive agency to

> "Establish a management control process to assure that appropriate administrative, physical, and technical safeguards are incorporated into all new computer applications and significant modifications to existing computer applications,"

it does not identify the specific controls necessary to ensure a reasonable level of protection for personal, proprietary, and other sensitive information. For example, the memorandum does not identify or describe the specific types of controls considered to be administrative, physical, or technical nor the circumstances under which it is best to use one type of control versus another.

In the absence of specific guidance, the executive agencies have found their ability to establish a reasonable level of protection for sensitive information to be confusing. A survey performed by NCSC in November 1980 found that only 30 percent of the executive agencies cited Transmittal Memorandum No. 1 as the source of authoritative basis to enable the establishment of controls over personal, proprietary, and other sensitive information.

An example of insufficient guidance in Transmittal Memorandum No. 1 is on the control of information subject to the Privacy Act of 1974 and the Freedom of Information Act.

Information disclosure requirements of the Privacy and Freedom of Information Acts must be considered when developing information security systems

Information disclosure requirements established by the Privacy and Freedom of Information Acts are complex and interrelated. In an earlier report, 1/ we stated that the basic problem

> "* * * is how to translate the broad social goals of privacy and fair information practice legislation into precise steps which computer scientists and managers of automated systems may follow in order to achieve acceptable levels of performance." (Emphasis added.)

1/"Automated Systems Security--Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data" (LCD-78-123, Jan. 23, 1979).

APPENDIX III

Transmittal Memorandum No. 1 does not translate the broad social goals of privacy (The Privacy Act of 1974) and fair information practice (The Freedom of Information Act) into precise steps for use in designing, developing, implementing, operating, and maintaining a total system of controls to prevent unauthorized disclosure of information.

The Congress intended these two acts to work together generally to ensure citizens their rights to access of Government records and to personal information, balanced against the Government's need to maintain confidentiality in appropriate circumstances.

The Privacy and Freedom of Information Acts provide much latitude to individual agencies as to how these goals should be implemented. However, in striking the balance between the need to safeguard individual privacy and the public interest in access to Government information, Transmittal Memorandum No. 1 should provide policy and guidance to executive agencies on how to establish adequate administrative, physical, and technical controls to protect against unauthorized disclosure. The lack of comprehensive criteria has generally resulted in significant differences in the information protection policies and procedures promulgated and in the degree they are implemented by the agencies. We found similar types of personal and sensitive information receiving a wide range of protection depending, to a considerable degree, on agency practice rather than the need for protection.

Confronted with the lack of guidance in Transmittal Memorandum No. 1, it is understandable that agencies have been generally confused about what constitutes an appropriate information security program and the level of security needed to protect various personal and other sensitive information. Many agencies informed us this condition was the reason they have taken little or no action to develop an effective information security program.

These problems essentially exist today, even though the Paperwork Reduction Act of 1980 provides a mechanism for OMB to ensure a leadership role to address and resolve these and related issues. As described in appendix IV, OMB has yet to assume its leadership role as specified in that legislation.

INFORMATION CLASSIFIED FOR PURPOSES OF NATIONAL SECURITY

Each executive agency head's responsibility for ensuring security of all agency information also includes information classified for purposes of national security. Transmittal Memorandum No. 1 does not define the term "national security information." Nor does the memorandum describe its interrelationship with other orders, directives, and laws that are intended to ensure an adequate level of protection is established for this type of information.

For example, Executive Order 12065 of June 28, 1978, is intended to balance the public's interest in access to Government information with the need to protect certain national security information from disclosure. Except as provided in the Atomic Energy Act of 1954, this order provides the basis for classifying information and the executive policy for safeguarding information classified for purposes of national security.

Transmittal Memorandum No. 1 does not provide clarification for determining when personal, proprietary, or other sensitive information should be considered for classification under Executive Order 12065. Transmittal Memorandum No. 1 makes the head of each executive agency responsible for establishing administrative, physical, and technical safeguards required to adequately protect personal, proprietary, and other sensitive information not subject to national security regulations. However, the memorandum does not clarify the conditions under which personal, proprietary, and other sensitive information must be afforded the same level of protection against unauthorized disclosure as they do information classified for purposes of national security. This situation has left many executive agencies confused as to the level of protection that is to be afforded personal, proprietary, and other sensitive information.

Some executive agencies are confused over what level of security sensitive information requires

Transmittal Memorandum No. 1 states that it "* * * promulgates policy and responsibilities for the development and implementation of computer security programs by executive branch departments and agencies." However, executive agencies are also governed by executive orders, public laws, and intelligence community directives which pertain to safeguarding information classified for purposes of national security. In agencies associated with the intelligence community it is not uncommon to provide generally the same level of protection over all agency information. In other words, access to sensitive information may be restricted in the same manner as access to classified information.

In agencies not associated with the intelligence community, however, certain kinds of personal, proprietary, and other sensitive information need to be afforded a level of protection against unauthorized disclosure equal to national security information. In the absence of specific direction in Transmittal Memorandum No. 1, some executive agencies are confused over whether to treat all agency information as if it were classified for purposes of national security or to establish less restrictive controls against unauthorized disclosure for information not classified for that purpose.

We believe that as a minimum, OMB must clarify the preferred sources of guidance and prioritize the circumstances where each is to be used.

APPENDIX III

SPECIFIC GUIDANCE LACKING FOR SYSTEMS USING TELECOMMUNICATION NETWORKS

As described in appendix II, automated information systems particularly those using telecommunication networks, are highly vulnerable to being misused for fraudulent, wasteful, abusive, and illegal purposes. Transmittal Memorandum No. 1 does not contain direction and/or guidelines for assessing telecommunication network vulnerabilities in the agency's automated information security program. We believe, this situation is unacceptable because, as we previously described in appendix II, executive agencies are making greater and greater use of telecommunication networks to link together their automated information systems.

To establish a reasonable level of protection over personal and other sensitive information requires the creation and maintenance of a total system of controls which must incorporate controls over both automated information systems and related telecommunication networks. This is not the first time we have reported on this issue. In 1980 1/ we reported that:

> "We reviewed five civil agency reports to OMB in response to Circular A-71, Transmittal Memorandum No. 1. These reports showed that the agencies' programs did not provide for assessing telecommunications vulnerabilities and including the impact of vulnerabilities on the data processing system safeguards and controls. Generally, agency officials responsible for data telecommunications security that we interviewed believed that their safeguards and controls for computer facilities, including remote user terminals, met OMB Circular A-71, Transmittal Memorandum No. 1, requirements for protecting data within their data processing systems. However, safeguards and controls for protecting computer facilities often do not protect against vulnerabilities in telecommunications networks supporting such systems. Therefore, we believe that agency programs for assessing safeguards and controls of a total automated information system should specifically address the data telecommunications portion of the system."

As we stated in our 1980 report,

> "OMB officials did not believe that additional guidance on telecommunications was needed to assist Federal agencies in implementing comprehensive security programs for automated information systems. However, they

---

1/"Increasing Use of Data Telecommunications Calls For Stronger Protection and Improved Economics" (LCD-81-1, Nov. 12, 1980).

APPENDIX III

did agree that data telecommunications networks, which are primarily vehicles for transmitting personal and other sensitive information within and between civil government agencies and among these agencies and the private sector, could significantly affect the adequacy of safeguards agencies are planning for the data processing portion of their automated information systems."

Since automated information systems in some executive agencies have been subjected to fraudulent, wasteful, abusive, and illegal practices (see app. II), we believe OMB guidance should address the level of security needed in telecommunication networks.

CENTRAL AGENCIES HAVE NOT BEEN EFFECTIVE IN FULFILLING THEIR INFORMATION SECURITY PROGRAM RESPONSIBILITIES

The four central agencies with Government-wide information security program responsibilities are OMB, Department of Commerce (particularly NBS), GSA, and OPM.

Collectively, these agencies have the responsibility for establishing the necessary policies, principles, standards, and guidelines that must be implemented by the executive agencies to have an efficient and effective information security program. The specific responsibilities of the central and executive agencies are described in OMB Circular A-71, Transmittal Memorandum No. 1, and the Brooks Act (Public Law 89-306). Additional responsibilities for OMB, GSA, and other executive agencies have been provided under the Paperwork Reduction Act of 1980.

The central agencies have not been effective in fulfilling their information security program responsibilities because (1) they have produced uncoordinated policies, principles, standards, and guidelines that some executive agencies have found to be confusing and (2) OMB has not assumed its leadership role as set forth in the Paperwork Reduction Act of 1980 or worked effectively with the executive agencies to ensure their implementation of Government-wide policy and guidance.

The responsibilities and action taken by each of the central agencies are briefly described in the following paragraphs.

OMB

OMB has a basic responsibility for establishing Government-wide fiscal and policy control over the executive agencies. Among other things, OMB is responsible for assisting the President in his program to develop and maintain effective Government by reviewing the organizational structure and management procedures of the executive branch to ensure that they are capable of producing the intended results.

With regard to executive automated information systems including security programs, OMB's responsibilities are described in the Paperwork Reduction Act of 1980. Transmittal Memorandum No. 1 requires the central agencies and the executive agencies to submit to OMB for review their plans and associated resource estimates for implementing an information security program. The central agencies were to submit their plans within 60 days of the date of the memorandum (July 27, 1978), while other executive agencies were allowed 120 days.

The Paperwork Reduction Act of 1980 broadened OMB's information security program responsibilities as part of its

leadership role in information resource management. Specifically, the Director of OMB was made responsible for

"(1) developing and implementing policies, principles, standards, and guidelines on information disclosure and confidentiality, and on safeguarding the security of information collected or maintained by or on behalf of agencies (emphasis added);

"(2) providing agencies with advice and guidance about information security, restriction, exchange, and disclosure; and

"(3) monitoring compliance with section 552a of title 5, United States Code [Privacy Act of 1974], and related information management laws.

"The Federal automatic data processing and telecommunications functions of the Director shall include

"(1) developing and implementing policies, principles, standards, and guidelines for automatic data processing and telecommunications functions and activities of the Federal Government, and overseeing the establishment of standards under section 111(f) of the Federal Property and Administrative Services Act of 1949 [as amended by P.L. 89-306, often called the Brooks Act];

"(2) monitoring the effectiveness of, and compliance with directives issued pursuant to sections 110 and 111 of such Act of 1949 and reviewing proposed determinations under section 111(g) of such Act 1/ (emphasis added);

"(3) providing advice and guidance on the acquisition and use of automatic data processing and telecommunications equipment, and coordinating, through the review of budget proposals and other methods, agency proposals for acquisition and use of such equipment;

"(4) promoting the use of automatic data processing and telecommunications equipment by the Federal Government to improve the effectiveness of use

---

1/Section 110 establishes a Federal telecommunications fund for use by executive agencies as provided in Public Law 87-847. Section 111 was added by the Brooks Act. The Brooks Act specifies the roles of OMB, GSA, and NBS in purchasing and operating Federal automated data processing systems.

and dissemination of data in the operation of Federal programs; and

"(5) initiating and reviewing proposals for changes in legislation, regulations, and agency procedures to improve automatic data processing and telecommunications practices, and informing the President and the Congress of the progress made therein." (Emphasis added.)

The Paperwork Reduction Act also states that OMB will within 2 years after the effective date of the act develop a program to (1) enforce Federal information processing standards, particularly software language standards, at all Federal installations and (2) revitalize the standards development program.

OMB's review of executive agency information security program plans

OMB assembled a small, multidisciplined task team of four persons, each from a different agency, to review the information security plans submitted by the agencies in accordance with Transmittal Memorandum No. 1 requirements. The task team met in December 1978 and developed a list of criteria to evaluate agencies' plans.

The task team's evaluations of agencies' plans showed substantial differences existed in how agencies interpreted the memorandum's requirements and approaches to strengthening their information security. OMB decided further clarification and action was needed. As a result, the task team developed an agency information security program checklist. The checklist was sent to the executive agencies in January and February 1979, and the agencies were requested to resubmit plans to OMB, in conformity with the checklist, by February 28, 1979.

The first task team disbanded after developing the information security checklist, so OMB assembled a new team to evaluate the second set of security plans. The second plans, however, were evaluated primarily by one individual. (A second individual helped for 2 weeks but was then recalled to the parent agency.) Working mainly alone, the evaluator critiqued the second responses from March through December 1979. The critiques were sent to the respective departments and agencies and identified those areas in the plans that the evaluator believed needed additional attention. The two most frequently identified weaknesses were the lack of provisions for personnel security (that is, screening of individuals participating in the design, operation, or maintenance of information systems) and inadequate contingency plans.

Also, OMB issued on October 28, 1981, Circular No. A-123, Internal Control Systems, which prescribes policies and standards to be followed by executive departments and agencies in establishing and maintaining internal controls in the program and

administrative activities. Specific guidelines for automated data processing internal controls have been prepared by OMB and are currently being reviewed for issuance to Federal agencies.

Our current evaluation shows that other than issuing circulars, OMB has not taken any further action to ensure the executive agencies' effective implementation of their information security program plans.

OMB's fulfillment of other Paperwork Reduction Act responsibilities

As provided for in the Paperwork Reduction Act, OMB created an Office of Information and Regulatory Affairs to fulfill the responsibilities of the Director of OMB. Other than recently drafting changes on internal control and reorganizing OMB's Information Systems Policy Division into this new office, not enough has been done to fulfill OMB's information security program responsibilities described in the act.

For example, the Paperwork Reduction Act makes the Director of OMB responsible for initiating and reviewing proposals for changes in executive agency procedures to improve information practices in those agencies. OMB is also responsible for monitoring the effectiveness of and the executive agencies' compliance with Government-wide policies, principles, standards, and guidelines for automated information security. OMB has yet to fulfill these responsibilities. Thus, OMB's limited implementation of its responsibilities has contributed to the executive agencies' automated information systems remaining highly vulnerable and subjected to fraudulent, wasteful, abusive, and illegal practices.

OMB's failure to assume its leadership role is in direct contrast to its response to our 1979 report when OMB stated that it was placing high priority on efforts during 1980 to improve security programs in the executive agencies. OMB's inaction does not support the President's program for reducing fraud and waste in the Government.

NBS

Under the Brooks Act, the Secretary of Commerce is responsible for "appropriate recommendations to the President relating to the establishment of uniform Federal automated data processing standards." The Secretary of Commerce has delegated this responsibility to NBS.

In 1978 NBS planned to issue 36 standards it considered necessary to achieve a reasonable level of protection over executive agencies' automated information systems. However, NBS has only issued six guidelines and one standard addressing various aspects of information security. Although these guidelines and standards are not as yet all inclusive of those needed to implement

and maintain a cost-effective information security program, their implementation by the executive agencies would reduce the level of vulnerability presently associated with their information systems. NBS encourages executive agencies to comply with these guidelines and standards, but does not thoroughly coordinate or cross-reference them with those of GSA and OPM on the same subject. Many officials we spoke with in the executive agencies have not placed much emphasis on implementing existing Government-wide policies, standards, and guidelines.

To further fulfill its responsibilities, NBS is continuing to develop additional and needed standards and guidelines on information security for use by the executive agencies. However, close coordination with OMB, GSA, and OPM will be necessary to ensure their maximum usefulness to the agencies who must use the guidance to achieve a reasonable level of protection over their automated information systems.

GSA

Although GSA has taken some action to fulfill its responsibilities as required by Transmittal Memorandum No. 1, we found no evidence to show it has adequately considered and cross-referenced its regulations with those of NBS and OPM on the same subject.

Transmittal Memorandum No. 1 required GSA to issue policies and regulations for the physical security of computer rooms and to ensure that agency procurement requests for computers, software, and related services include appropriate security requirements. GSA sent its plans for meeting the memorandum's requirements to OMB on October 11, 1978, and on November 24, 1978. In the November plan, GSA discussed its intention to revise the Federal Procurement Regulations and the Federal Property Management Regulations to include the requirements, and it established March and April 1979 as the target completion dates for these revisions.

GSA has drafted, circulated for comment, evaluated, and incorporated comments on three revisions: Federal Property Management Regulations 101-35.3 series on the security of Federal automated data processing and telecommunications, Federal Property Management Regulations 101-36.7 series on environment and physical security, and Federal Procurement Regulations 1-4.11 on security requirements for Federal agencies and Government contractors.

GSA did not send out the request for comments until October 1979, and the Federal Property Management Regulations above became effective in August 1980. GSA officials, however, attributed the delay in reaching their targeted completion dates to the "wider than originally planned" audience asked to comment on the draft revisions. (Less than 40 recipients were initially targeted, but the final distribution for comments comprised almost 500 names and organizations.)

GSA is responsible for establishing the guidance for other agencies in certain automated data processing procurement and management areas. Recently, GSA has conducted some reviews of agency actions to determine compliance with regulations and conditions of procurement delegation. Such reviews, if directed toward information security and performed with sufficient regularity, could ensure substantial compliance on a Government-wide basis. However, the reviews have not been performed to determine compliance with regulations and conditions of procurement delegation for information security. Thus, they are not sufficient in scope to assist the agencies in establishing a reasonable level of protection over their information systems.

OPM

OPM has issued some guidelines on selected aspects of the information security program as required by Transmittal Memorandum No. 1. The memorandum required OPM to establish personnel security policies for Federal personnel associated with or having access to data in Federal computer systems. OPM's October 26, 1978, response to OMB included Federal Personnel Management Letter 732-7 on a "Personnel Security Program for Positions Associated with Federal Computer Systems." The letter's requirements became effective on November 14, 1978, and presented guidelines agencies must use when establishing their personnel security programs. Three sensitivity designations--developed, in part, from then-existing OPM guidance--were presented as a basis for determining what level of investigation should be made on personnel working in a computer systems environment. Furthermore, OPM made allowances to "grandfather" or accept current information processing employees as exempt from background investigations if they had at least 1 year of satisfactory work experience. This had the effect of giving employees security approvals without a thorough background investigation.

Federal Personnel Management Letter 732-7 indicated that OPM's authority did not permit extending the letter's coverage to Government contractor employees and that agencies would have to prepare their own policies to handle such situations. A number of agencies, however, questioned whether authority existed for them to screen and investigate contractor employees who would not have access to classified data. Acting on the agencies' concerns, OPM requested and received an opinion on the issue from the Department of Justice. OPM subsequently issued Federal Personnel Management Bulletin 732-2, dated January 11, 1980, summarizing the Department of Justice's opinion that Federal agencies have the authority to screen contractor employees as long as it is done consistent with the due process of law. Even though this issue was subsequently resolved, certain agencies may not be in compliance. For example, an agency official stated that his agency would not take the initiative to investigate contractor employees.

APPENDIX IV

EVALUATION OF CENTRAL AGENCY ACTIONS TO FULFILL INFORMATION SECURITY PROGRAM RESPONSIBILITIES

There is no question that executive agencies' automated information systems have been subjected to fraudulent, wasteful, abusive, and illegal practices. Losses have run into the millions of dollars. Resolution of this problem requires strong positive action by central and executive agencies. OMB should develop and monitor sufficiently detailed policy, standards, and guidelines necessary to implement and maintain a cost effective and reasonable level of protection over the Government's automated information systems.

OMB has not effectively assumed its leadership role as set forth in the Paperwork Reduction Act of 1980, particularly that portion applicable to information security programs.

Although OMB has issued Transmittal Memorandum No. 1 in partial fulfillment of its broader responsibilities, it has not taken adequate action to oversee its effective implementation by executive agencies. The Paperwork Reduction Act requires OMB to initiate proposals for changes in agency procedures to improve information practices in the executive agencies and to report to the President and the Congress on the progress made therein. OMB has yet to fulfill this responsibility.

In 1978 NBS planned to issue 36 standards it considered necessary to achieve a reasonable level of protection over automated information systems. As of January 1982, six guidelines and one standard had been issued. This is far short of those needed and leaves the executive agencies without needed guidance for implementing and maintaining cost-effective information security systems.

As indicated above, GSA has issued three revisions to its Government-wide regulation, but like the other central agencies, it has not taken an adequate role to ensure executive agencies comply with them. As a result, little action is taken by executive agencies to implement Government-wide information security policies, principles, standards, and guidelines.

The original OPM guidance to agencies left unanswered questions, such as the impact on information security programs of employees with clearances for access to personal, proprietary, and other sensitive information who obtained them without background investigations and how to treat contractor personnel. Although the investigation of the contractor personnel issue was later solved, OMB, in accordance with its monitoring responsibilities under the Paperwork Reduction Act of 1980, has not assured itself executive agencies are in compliance.

The Government is placing more sensitive information in automated information systems and the vulnerabilities are greater

APPENDIX IV

unless a reasonable level of protection is provided. Consequently, the lack of emphasis by the central agencies in fulfilling their information security program responsibilities has left the Government's automated information systems even more vulnerable to fraudulent, wasteful, abusive, and illegal practices than they have been in earlier periods.

APPENDIX V

SENIOR MANAGEMENT GIVES ONLY LIMITED SUPPORT TO AUTOMATED INFORMATION SECURITY PROGRAMS

It is well recognized that senior management in the executive agencies has the primary responsibility for establishing and maintaining a cost effective and reasonable level of protection over their automated information systems. However, (1) executive agencies are doing very little to implement information security programs and (2) many senior managers are not fully aware of how highly vulnerable their systems are to fraudulent, wasteful, abusive, and illegal practices.

The establishment and maintenance of the needed level of protection involves implementing a cost-effective total system of controls. A total system of controls consists of three general categories of controls--administrative, physical, and technical. The nature and extent of the controls needed are dictated by the type of information; its sensitivity; the environment; the equipment, including telecommunication networks; the facilities; the software; and the people involved. Depending on the degree of vulnerability to natural disaster; human error; and fraudulent, wasteful, abusive, and illegal practices, the amount of risk associated with that system may be either acceptable or unacceptable. A technique known as risk analysis (see Federal Information Processing Standard 65) is used to ascertain the extent to which an information system is highly vulnerable to natural disaster, human error, and improper or illegal use. Other factors that can have a bearing on executive agencies' effectiveness in ensuring information protection are personnel security practices, contingency planning, system redundancy, audit practices, and the organizational structure and environment.

Our evaluation showed that executive agencies do not generally use risk analysis techniques or other forms of sound administrative, physical, or technical controls, such as employee background investigations, contingency planning, ensuring the availability of backup equipment and software for use in event of a natural or deliberate disaster, or even providing for systematic internal reviews.

RISK ANALYSIS TECHNIQUES NOT GENERALLY USED

Transmittal Memorandum No. 1 requires executive agencies to:

> "Assign responsibility for the conduct of periodic risk analysis for each computer installation operated by the agency, including installations operated directly by or on behalf of the agency. The objective of this risk analysis should be to provide a measure of the relative vulnerabilities at the installation so that security resources can effectively be distributed to minimize the potential loss. A risk analysis shall be performed:

"(1) Prior to the approval of design specifications for new computer installations.

"(2) Whenever there is a significant change to the physical facility, hardware or software at a computer installation. Agency criteria for defining significant changes shall be commensurate with the sensitivity of the information processed by the installation.

"(3) At periodic intervals of time established by the agency, commensurate with the sensitivity of the information processed by the installation, but not to exceed five years, if no risk analysis has been performed during that time."

Most executive agencies generally selected, implemented, and maintained a system of controls based on limited personal insight rather than using risk analysis techniques. Risk analysis techniques provide a basis for management to implement and maintain a total system of controls which considers the cost effectiveness of protecting the information versus the risks associated with its misuse for fraudulent, wasteful, abusive, and illegal purposes. The selection, implementation, and maintenance of controls based on limited personal insight does not provide a means for viewing an information system from a total system perspective.

During our evaluation, we did not find any executive agency performing a comprehensive risk analysis, although there was one agency that performed risk analyses for only selected components of a computer system but not from a total system's perspective. For a risk analysis to accurately isolate needed controls, the analysis must be developed from an overall system's perspective. The overall system's perspective includes a review and evaluation of the processes involved in the origination of information through its final use or destruction.

Transmittal Memorandum No. 1 requires executive agencies to perform a risk analysis whenever a significant change is made to computer facilities, equipment, or software. The memorandum also requires the agencies to establish criteria for determining the type of change that will be considered as significant. In some instances, we found that executive agencies have yet to establish criteria for defining a significant change. Without such criteria, for example, one agency is yet to perform a risk analysis even several months after relocating its computer center to another building in the same city.

Without performing a risk analysis, which is an essential first step in developing an information security program, many Federal agencies' information security programs remain unnecessarily vulnerable to accidental abuse and deliberate acts of sabotage, fraud, waste, and other forms of inefficiency.

PERSONNEL BACKGROUND INVESTIGATIONS GENERALLY NOT PERFORMED

OPM has developed criteria for making investigations of Federal employees and contractors associated with the design, operation, or maintenance of Federal computer systems or having access to information in Federal computer systems through two Federal Personnel Manual letters or bulletins. However, as mentioned in appendix IV, agencies were allowed to grandfather Federal employees with 1 or more years of satisfactory service in an automated data processing position. This avoided the requirement for performing background investigations because those personnel were exempted from the background investigations.

During our evaluation we noted that only one executive agency had made background checks and classified the employees and contractor positions according to the three security levels required by OPM. The security officers at two agencies did not have extensive background investigations completed for themselves, even though both occupied positions defined by OPM as being highly sensitive because the agencies that employed them had not defined their positions in accordance with OPM guidance.

Background investigations are necessary because employees or contractors who have access to the systems (i.e., designers, programmers, operators, and users) are major potential threats to sensitive information. These individuals have (1) programming skills and (2) understanding of complex systems and knowledge of weaknesses in the design and implementation of the system. The potential for misuse of information by individuals in positions of trust is not unique to automated information processing systems--the problem exists in manual systems as well. Nevertheless, the concentration of information in automated systems increases the magnitude of the risks over computerized systems, and additional controls are necessary.

RELIABLE CONTINGENCY PLANNING LACKING

Federal agencies have done little to develop contingency plans to counter the possible loss of their automated information systems. Agencies must be able to maintain continuity of operations after a disaster occurs. Several agencies provide offsite storage for master files for duplicate information or reconstruction of information in the event of a disaster. However, the majority do not have sufficient backup hardware and software.

Contingency plans for emergency response, backup operations, and postdisaster recovery are required by OMB's Transmittal Memorandum No. 1. Contingency plans will not result in the duplication of all the features from the original operating environment. However, these plans can assist in providing a capability to continue key operations after a disaster occurs, such as a fire, power failure, flood, or even vandalism.

Almost 70 percent of the agency officials we interviewed responded that their agency had established policies and assigned responsibilities for preparing and maintaining contingency plans. However, we found that not every one of these agencies had in fact developed such a plan. The "plans" we evaluated were inadequate because they did not provide for effective backup capabilities and were therefore not real contingency plans.

Nearly two-thirds of the officials we interviewed did not know if their "contingency plans" were reviewed and tested at periodic intervals. A contingency plan that is not tested at periodic intervals is of little or no value because there is no assurance it can be implemented when disaster occurs. In our December 18, 1980, report (AFMD-81-16), we said "* * * in the 55 Federal activities we reviewed, we did not find a single agency ADP backup plan which we consider adequate." Those conditions appear to have changed little since that time.

BACKUP SOFTWARE AND HARDWARE NOT AVAILABLE

Agency officials' primary concern for contingency planning is to be certain that compatible hardware and software are available at the backup location. However, we found many cases where management has not thoroughly considered the requirement to provide needed backup and recovery capabilities for their operating software. Operating software controls the processing of application programs--instructions to do a specific job such as payroll or personnel recordkeeping. Operating software on backup computers must be compatible with the operating software on the agency's computers. Agencies with differing operating software will have a difficult time trying to use backup hardware because their application programs will not be executed or executed correctly.

Obtaining backup from a commercial source is an option. There are several companies that can provide this service; however, the costs should be carefully evaluated with respect to the benefits.

For example, the Bureau of the Census had modified its UNIVAC computer operating system and had special programs built to process its input and output applications. On August 8, 1979, when Census experienced flooding in its computer facility, all of its computers suffered water damage. No other Federal or commercial center could provide ready computer backup without dedicating their entire computer to the Census Bureau. Consequently, to process their high priority applications, Census had to acquire dedicated computer time commercially until its own computer equipment was restored. The cost of leasing and operating this equipment was estimated in our report at more than

$1.5 million. 1/ In 1981 we reported that automated data processing security and backup recovery capabilities for continuity of operations remained a problem in the Bureau. 2/

SENIOR MANAGEMENT PROVIDES LIMITED SUPPORT FOR INTERNAL REVIEW

Internal review functions relating to information systems and information security programs include (1) a review of systems planning and performance, (2) financial reviews of budget development, submission, and approval, (3) reviews of administrative, physical, and technical controls, and (4) a variety of related functions, such as evaluation of plans for maintaining continuity of computer operations during an emergency or following a disaster. This list should not be considered all-inclusive; only illustrative of the functions performed by an internal review group.

These reviews should be performed by an organization independent of the user organization and computer/communications facility managers, such as the Inspector General's office or the agencies' internal audit group, and information security offices. In general, we found that little is being done to perform effective internal reviews, in part, because senior management has only provided limited support for this vital function. As a result, senior management has little or no means to determine how vulnerable its information systems are and the magnitude of the risks associated with those systems. Those officials responsible for making internal reviews said that senior management has been reluctant to allocate sufficient time and resources for them to properly perform the needed internal review function. Other examples of problems experienced in evaluating information systems are contained in a more detailed report we issued in 1981. 3/

For these reasons, the range of involvement of internal review staffs in evaluating their agencies' information systems varies from limited involvement to constant surveillance by some information security officers.

1/"Most Federal Agencies Have Done Little Planning for ADP Disasters" (AFMD-81-16, Dec. 18, 1980).

2/"The Bureau of the Census Must Solve ADP Acquisition and Security Problems" (AFMD-82-13, Oct. 31, 1981).

3/"Federal Agencies Still Need to Develop Greater Computer Audit Capabilities" (AFMD-82-7, Oct. 16, 1981). See also "Computer Auditing in the Executive Departments: Not Enough Is Being Done" (FGMSD-77-82, Sept. 28, 1977). "GAO Findings on Federal Internal Audit--A Summary" (FGMSD-80-39, May 27, 1980).

APPENDIX V

THE INFORMATION SECURITY FUNCTION GENERALLY ORGANIZATIONALLY MISPLACED

To be effective, the information security function must be organizationally located so that it functions independently of line management and reports directly to senior management.

The security function is organizationally misplaced in some agencies because the security officers lack independence. For example, at one agency the security officer reported directly to the computer processing line manager. This caused information security to be in competition with the agency's operational priorities. In several agencies, operating priorities override security requirements. Serious security problems result, leaving the information systems highly vulnerable to misuse and abuse.

One information security officer said that his recommendations for improving system controls were not seriously considered by the computer processing line management that he reported to. This agency moved its computer facility to a new location that failed the security officer's preinstallation inspection. For example, physical controls at the new location cannot provide proper protection for certain types of vulnerabilities known to exist at the new location. However, the agency is using the facility without making all the needed corrections to eliminate or minimize the risks directly associated with those vulnerabilities.

MANY SENIOR MANAGERS ARE NOT FULLY AWARE OF HOW VULNERABLE THEIR INFORMATION SYSTEMS ARE

Since risk analysis techniques are not generally used in executive agencies, senior management is unaware of how vulnerable their information systems really are to unauthorized and illegal practices.

Our evaluation showed that information security programs receive little in the way of financial and budgetary support from senior management. The limited support provided by senior management is evidenced by (1) the limited resources committed to and used for risk analysis, (2) failure to define their data processing operations in accordance with the OPM criteria for personnel security programs, (3) failure to provide reliable contingency and backup capabilities for their automated data processing operations, including backup hardware and software, and (4) a failure to provide an appropriate separation of duties between information security officers and data processing managers.

A total system of controls must be developed, implemented, and maintained to achieve a reasonable level of protection over personal, proprietary, and other sensitive information. Risk analysis techniques are used to identify the specific controls needed to provide a reasonable level of protection from a total system perspective. The most cost-effective way to incorporate

those controls into a system is when it is being designed. The cost of retrofitting the needed software controls into a large-scale system once it is placed into operation is at least 30 times the cost to incorporate the same controls during the design phase.

As described in appendix II, the nature of the information security problem is highly complex and technical. Most senior managers in the executive agencies are not aware of the highly complex and technical issues associated with their information security problems because they lack needed information from thorough risk analysis techniques and internal reviews. As a result, they have seen little reason to provide the needed financial and budgetary support to develop and maintain a reasonable level of protection over personal, proprietary, and other sensitive information.

- - - -

As illustrated by the foregoing examples, senior management is giving only limited support to the automated information security program, even though the information systems have been subjected to fraudulent, wasteful, abusive, and illegal practices. With the executive agencies' rapid increase in the use of telecommunication networks to link their information systems, those systems are becoming even more vulnerable to such improper practices than in the past.