Chapter 4

Information Systems Security

Contents

Tables

Chapter 4

Information Systems Security

SUMMARY

This chapter examines needs and policies for the protection of Federal data and information systems from a variety of problems, ranging from technical failures to unauthorized use or manipulation of data.

Concerns about the security of information systems began to become prominent in the mid to late 1960s, particularly in military and national security agencies of the government. Generally, while the Department of Defense (DOD), and particularly the National Security Agency (NSA), has developed a great deal of technical expertise in this area, the civilian agencies have lagged in awareness. In the last decade, however, concerns about both privacy and hackers have elevated the overall visibility of this issue.

The basic policy document for government-wide information security is the Office of Management and Budget (OMB) Circular A-130 issued in December 1985 (replacing Circular A-71, Transmittal Memorandum No. 1, issued in 1978), which requires agencies to designate security officers, conduct risk analyses, and take other appropriate steps to protect their information systems. In September 1984, the White House issued National Security Decision Directive 145 (NSDD 145), which essentially attempts to bring together the separate paths of civilian and military information systems security, with NSA serving as a resource and coordinating point for all national security-related applications in the Federal Government. The scope of NSDD 145 and NSA's authority is based on a definition of "information sensitive for national security reasons" which has not yet been worked out, but is likely to be far broader than classified information alone.

OTA's major findings in this area are:

- The government faces fundamentally new levels of risks in information security because of increased use of networks, increased computer literacy, an explosion in microcomputer use and decentralized data processing capabilities, and increased dependency on information technology overall.
- Although there has been some progress in the past 5 to 10 years, there is widespread evidence that Federal policy requiring the use of appropriate information systems security measures has been ineffective. The General Accounting Office (GAO) reports and the OTA Federal Agency Data Request indicate that agencies often are not taking the actions mandated by OMB Circulars A-71 and A-130, such as performing risk analyses and screening personnel who work with sensitive applications. For example, for systems that process sensitive but unclassified information, OTA found that about one-quarter of the agencies responding do not screen personnel, about one-half do not perform a management review of sensitive applications, and about 40 percent do not use audit software or restrictions on dial-up access for any of these systems. In addition, about 40 percent of agencies have not conducted a risk analysis in the last 5 years, about 75 percent do not have an explicit security policy for microcomputers, and about 60 percent do not have (and are not developing) contingency plans in the event of disruption of mainframe computers.
- Three key factors inhibit appropriate Federal information security measures: 1) competition for resources in Federal programs, which limits spending for a "latent" issue like security; 2) a lack of awareness or motivation among agency personnel and top management; and 3) an absence of clear guidance on appropriate security measures.

- As NSDD 145 is implemented, it becomes increasingly clear that NSA and the committees guiding its implementation will play a significant if not dominant role in all aspects of information security in the Federal Government, whether or not the information is classified. Thus, NSDD 145 is likely to result in stronger governmentwide leadership in information security policy; however, concerns have been expressed that it puts the national security community in an unusual influential, if not controlling, position on a key aspect of the Nation's information policy.
- Possible actions to improve Federal information systems security include: more intensive congressional oversight, changing budget procedures with information security receiving higher priority and visibility, designating a civilian agency to be responsible for security training and technical support in the nonmilitary sector of government, and revising and clarifying NSDD 145.

INTRODUCTION

This chapter and the next ("Chapter 5: Computer Crime") are closely tied, in that they both focus on the integrity of information systems, although they emphasize different aspects of the problem. There are four general kinds of measures to protect information systems: 1) technical measures, such as cryptography; 2) administrative measures, such as making sure disbursements cannot be authorized by only one person; 3) physical measures, such as locking up diskettes; and 4) legal remedies to discourage abuse and prosecute perpetrators. This chapter discusses primarily the technical, administrative, and physical security measures, while chapter 5 discusses computer crime legislation.[1]

Finally, though this chapter addresses information systems security considered broadly—including both computers and telecommunications—computer security is analyzed in more detail than telecommunications security. A related OTA study will provide further analysis of telecommunications security issues.[2]

[1]It should be noted that the management of information security is one important aspect of good overall information technology (or information resources) management. It is an axiom of the information technology management field that effective information security cannot be independent of other aspects of management, or relegated to technical security experts. Rather, the managers and users of information systems must consider security throughout the plarming, implementation, and use of the systems. Thus, although this chapter focuses its analysis on one goal of information technology management—security—it should be emphasized that good overall management and good security practices are intertwined.

[2]The study, "New Communication Technologies: Implications for Privacy and Security," is scheduled for completion in fall/winter 1986.

BACKGROUND

Attention began to focus on the security of unclassified information systems in the Federal Government in the mid to late 1960s. Important factors that led to this concern include the development of multi-user ("resource sharing") computer systems, and the growing interest in privacy and government data banks.[3] In addition, a number of notorious computer crimes in the 1970s reinforced the fact that information systems do indeed have significant vulnerabilities.[4]

[3]An important early document is a report by the Defense Science Board Task Force on Computer Security, "Security Controls for Computer Systems," edited by Willis H. Ware. It was originally issued in classified form in 1967, and later declassified and published for the Office of the Secretary of Defense by Rand Corp., Santa Monica, CA, 1979. For more historical information see also L.G. Becker, Congressional Research Service, "Computer Security: An Overview of National Concerns and Challenges," report No. 83-135 SPR, Feb. 3, 1983.

[4]See U.S. Department of Justice, Bureau of Justice Statistics, *Computer Crime: Computer Security Techniques*, September 1982. The document was prepared by SRI International under a contract with the Department of Justice.

The threats and problems faced by computer systems include:[5]

1. Mistakes, both errors and omissions, that result in loss of data integrity. Examples: keyboard entry errors, programming errors, bringing magnets near storage media.
2. Dishonest employees with self-serving goals (usually economic) committing acts they prefer not to be noticed. Examples: "Data diddling" to generate unauthorized disbursements; using privileged information for personal gains.
3. Loss or disruption to data-processing capability from any cause. Examples: fire, flood, hurricanes, civil unrest, falling aircraft (for computer installations near airports), and loss of supporting services and facilities.
4. Disgruntled employees who commit damaging acts without economic or other self-serving goals. Examples: employees accessing information after they quit; destroying essential tapes; or planting "logic bombs" of various sorts, which disrupt the computer's operating system at a specified time.
5. Outsiders who, through some illicit act, accidentally or intentionally cause loss of data integrity or loss of or disruption to the means of processing those data. Examples: hackers gaining unauthorized access and/or tampering with files, industrial espionage via eavesdropping on data transmissions.

Table 4-1 lists some of the common measures that can be used to protect information systems from these problems. It is not exhaustive, but suggests the range of safeguards that are available. In order to match the value of data and the differing risks with appropriate safeguards, information security experts commonly use a technique known as risk analysis. It is a variant of risk analysis techniques that have gained prominence in the last two decades to help make decisions about environmental issues and other technological hazards.[6] In general, a risk analysis for an in-

Table 4.1.—Common Administrative, Physical, and Technical Information Security Measures

Administrative security measures:
- Background checks for key computer employees.
- Requiring authority of two employees for disbursements.
- Requiring that employees change passwords every few months, do not use the names of relatives or friends, and do not post their passwords in their offices.
- Removing the passwords of terminated employees quickly.
- Providing security training and awareness programs.
- Establishing backup and contingency plans for disasters, loss of telecommunications support, etc.
- Storing copies of critical data off-site.
- Designating security officers for information systems.
- Developing a security policy, including criteria for sensitivity of data.
- Providing visible upper management support for security.

Physical security measures:
- Locking up diskettes and/or the room in which microcomputers are located.
- Key locks for microcomputers, especially those with hard disk drives.
- Requiring special badges for entry to computer room.
- Protecting computer rooms from fire, water leakage, power outages.
- Not locating major computer systems near airports, loading docks, flood or earthquake zones.

Technical security measures:
- Audit programs that log activity on computer systems.
- Security control systems that allow different layers of access for different sensitivities of data (e. g., each level requires a different password).
- Encrypting data when it is stored or transmitted, or using an encryption code to authenticate electronic transactions.
- Techniques for user identification, ranging from simple ones such as magnetic stripe cards to more esoteric "biometric" techniques, which rely on hand or eye scanners (just beginning to be used).
- "Kernel' '-based operating systems, which have a central core of software that is tamperproof and controls access within the system.[a]
- "Tempest" shielding that prevents eavesdroDDers from picking up and deciphering" the signals given off by electronic equipment.[a]

[a]Generally used only in military or other national security applications

SOURCE Office of Technology Assessment

[5]Adapted from Robert H. Courtney, Jr., and Mary Anne Todd, "Problem Definition: An Essential Prerequisite to the Implementation of Security Measures, " paper prepared for presentation to the Second International Congress and Exhibition on Computer Security, Toronto, Sept. 10-12, 1984, p. 4. Courtney argues that these problems are listed in order of decreasing economic importance-i. e., that mistakes are the most important problem, and outsiders the least—although others would rank the problems differently.

[6]The National Science Foundation's Technology Assessment and Risk Analysis Program has funded and coordinated much of the pioneering work in this area. See, for example, V. Covello and M. Abernathy, "Risk Analysis and Technological Hazards: A Policy-Related Bibliography, " National Science Foundation (mimeograph), 1982; National Research Council, Committee on Risk and Decision Making, *Risk and Decision Making: Perspectives and Research* (Washington, DC: National Academy Press, 1982).

formation system involves answering the following questions:

1. What are the threats or vulnerabilities that this system faces?
2. How likely are those threats or vulnerabilities?
3. What would be lost?
4. What are the alternatives for protecting against these threats, and how does the cost of the alternatives compare with the size and likelihood of losses if the system is not protected?

OMB'S Circular A-130 (and its predecessor, Circular A-71, Transmittal Memorandum No. 1) requires risk assessments for information systems at least every 5 years, although it does not specify what constitutes a risk assessment or an information system. Risk analysis techniques for information systems range from an informal and brief qualitative procedure for a small microcomputer system, to a highly quantitative, in-depth examination of a major computing center. The latter are typically performed by a consultant for $50,000 to $250,000 and up. In the past few years, several vendors and research labs have developed risk analysis procedures that are automated and can be considerably cheaper.[7]

A risk analysis technique published by the National Bureau of Standards (NBS) in 1979 is the basis of many risk analyses performed in government and in the private sector. The procedure, published in Federal Information Processing Standards Publication 65, involves identifying potential threats, and then developing an "annualized loss expectancy" for each threat. For example, one might estimate that a fire in the tape storage room would cause $300,000 in losses (e.g., including damage, denial of use, and possible disclosure), that it would occur (within an order of magnitude) once every 30 years, and that the resultant annualized loss estimate was $10,000 (i.e., $300,000/30). Once annualized loss estimates are determined using this system, one can compare them to the costs of implementing protective measures. For example, the cost for afire control system for the tape storage room, amortized over its expected lifetime, might be $5,000 per year. If so, the analysis would suggest that such a system ought to be considered.

Although risk analyses modeled on the NBS system are widely used, they have distinct drawbacks. In particular, the process can become quite lengthy and include a great deal of personal judgment. Many critics have noted, for example, that estimating the frequency of events that have never occurred is particularly difficult. Thus, simpler and less quantitative techniques for risk analysis are becoming more popular, especially for smaller information systems. The U.S. Geological Survey (USGS), for example, uses a questionnaire-based system to identify possible risks and to determine whether appropriate protective measures have been considered. Table 4-2 provides an example of the format. The principle behind the USGS system is to identify a set of baseline measures and to ensure that system managers have considered implementing them. They are thus informed and accountable for the security of their systems.

Federal Information Security

Though there are common aspects, there is wide variation among and within Federal agencies in the kinds of information technology they use, in the nature of their information security problems, and in their awareness of those problems. Even within agencies (e.g., DOD), different functions or installations will range from being at the cutting edge of sophistication in information security to very minimal awareness and protective measures. And clearly, the national security community is distinctly different from much of the rest of government in the threats it faces and in its sophistication with regard to computer security.

Largely because of this difference in sophistication, the military (including parts of civilian government that generate classified infor-

[7] See, for example, Suzanne Smith and J.J. Lim, Los Alamos National Laboratory, "A Framework for Generating Automated Risk Analysis Expert Systems," presentation at Federal Information Systems Risk Analysis Workshop, Montgomery, AL, Jan. 22, 1985.

Table 4-2.—illustrative ADP Security—Risk Assessment Questions

Site location —_____

Controls and procedures	Yes	Risk is acceptable	Corrective action
1. Has the responsibility for the protection of each and every ADP resource (computer system, data, programs, etc.) been explicitly assigned?	—		
2. Are procedures in place to inform employees what resources they are expected to protect and from what hazards, what variances they are to note, and what corrective action they are to take?	—		
3. Are procedures in place to ensure the timely and complete separation of terminated employees?	—		
4. Is there a policy consistent with generally accepted practice about who may access and update data?	—		
5. Where indicated by the sensitivity of the resource and size of user population, is the policy enforced by the system?	—		
6. Is each individual user of the system uniquely identified?	—		
7. Is there a procedure (e.g., password, magnetic-stripe card) to authenticate the identity of the individual user of the system?	—		
8. Are users restricted to only those resources (e.g., data sets, records or segments, fields, transactions, etc.) required for their job?	—		

SOURCE U S Geological Survey

mation) and civilian sides of government have taken different paths in responding to escalating security concerns. The military side has been pursuing information security (particularly telecommunications, but increasingly computer security also) for much longer than other parts of government. It has powerful institutions and a great deal of technical expertise in this area.[8] Much of this expertise has traditionally been centered in NSA, whose mission includes both gathering intelligence from international telecommunications transmissions, and protecting U.S. transmissions from interception, alteration, and disruption.

Beginning in the 1970s, the concern on the military side broadened into several major programs and Presidential directives for protecting national security information. A key milestone was President Carter's Presidential Directive/National Security Council-24 (PD-24), issued on February 16, 1979. The directive focused on developing telecommunications security safeguards for classified information as well as unclassified government and private sector information that would be "useful to an adversary." It gave joint responsibility to the Secretary of Defense (delegated to NSA) and to the Secretary of Commerce (delegated to the National Telecommunications and Information Administration (NTIA)) to monitor telecommunications security needs in government and the private sector, and to propose a national policy for cryptography.[9] Eventually, NTIA's role in information security was phased out during the Reagan Administration.

For unclassified information unrelated to national security, the motivations for addressing information security are quite different.

[8] See Sanford Sherizen, "Federal Computers and Telecommunications: Security and Reliability Considerations and Computer Crime Legislative Options," OTA contractor report, February 1985.

[9] Presidential Directive/National Security Council-24 (unclassified extract), "National Telecommunications Protection Policy," Feb. 16, 1979.

Rather than facing a sophisticated adversary who seeks to obtain protected information, civilian agencies (and many parts of the military agencies as well) face a diffuse set of problems, ranging from computer-related embezzlement of funds by employees to unauthorized use of sensitive personal or proprietary data, to simple errors and omissions. The pattern of policy development for protection of this kind of information has been similarly diffuse. In the late 1960s and early 1970s, congressional concerns about privacy led to the Privacy Act of 1974, which controls the collection and use of personal information by Federal agencies.

One of the most significant policy actions for governmentwide information security took place in 1978, when OMB issued Transmittal Memorandum #1 (TM-1) to its Circular A-71 on the management of Federal information technology. TM-1 requires agencies to implement a computer security program. This program includes: 1) designating a security officer for each installation, 2) establishing personnel screening procedures for those who work with sensitive computer systems, 3) establishing procedures for evaluating the sensitivity of applications and certifying that systems are appropriately secure, 4) performing periodic audits and risk analyses for each computer installation, and 5) establishing contingency plans for disruptions to information systems. The memorandum also assigns to Federal agency heads the responsibility for assuring appropriate levels of security in their information systems; and it directs the General Services Administration (GSA) and NBS to develop policy guidelines and standards for Federal information systems security.

Table 4-3 highlights the policy documents that represent the current policy framework for information systems security. In addition, individual agencies, particularly DOD and intelligence agencies, have information security policies that go beyond the governmentwide guidelines. See appendix 4A at the end of this chapter for some examples.

Since the early 1980s, there has been a resurgence of interest in information security problems and policies, both for national security-related and other Federal systems. Some of this interest is clearly tied to the recent incidents of computer "hackers" gaining unauthorized access to computer systems, ranging from the Memorial Sloan-Kettering Cancer Center to Los Alamos National Laboratory. Although hackers have often brought attention to computer security issues, they appear

Table 4-3.—Key Federal Policy Documents Affecting Information Systems Security

Brooks. Act of 1965 (Public Law 89.306):
Gives OMB and GSA joint authority to set policy on Federal information technology; Commerce/NBS provides supporting standards, research, and technical assistance.

Privacy Act of 1974 (Public Law 93.579):
Restricts collection and use of personal information by agencies; requires them to take precautions to prevent unintended disclosure of personal information.

OMB Circular A-71, Transmittal Memorandum #1, 1978:
Requires agencies to establish a computer security program, including periodic risk analyses, management certification of sensitive applications, and designation of computer security officers.

Presidential Directive/National Security Council-24 (PD-24), "National Telecommunications Protection Policy, " Feb. 16, 1979 (superseded by NSDD 145):
Gives Defense/NSA and Commerce/NTIA joint responsibility to monitor telecommunications security needs in government and private sector, and to propose cryptography policy. NTIA's role was ultimately phased out.

Paperwork Reduction Act of 1980 (Public Law 96.511):
Endorses the concept of information resources management, establishes the Office of Information and Regulatory Affairs at OMB, and charges that office with evaluating agency information management and setting and coordinating related policies.

Federal Managers Financial Integrity Act of 1982 Public Law 97.255):
Requires agencies to examine their internal control systems and report deficiencies and plans for correcting those deficiencies to the President and Congress.

National Security Decision Directive 145, "National Policy on Telecommunications and Automated Information Systems Security, " issued by the White House, Sept. 17, 1984:
Sets NSA as the focal point for both military and civilian information security related to national security. NSA is to assist an interagency committee (NTISSC) in developing and coordinating policies, evaluating computer and telecommunications security, and reviewing and (for telecommunications) approving budgets for computer and communications security efforts throughout government.

OMB Circular A-130, "Management of Federal Information Resources" Dec. 12, 1985 (supersedes A-71):
Reinforces provisions of A-71, updates A-71 to acknowledge microcomputers, Federal Managers' Financial Inteqrity Act, NSDD 145.

SOURCE Office of Technology Assessment

to be only a small part of the overall computer security problem. Security experts are nearly unanimous in their view that the more significant security problem is abuse of information systems by those authorized to use them, rather than by those trying to penetrate the systems from outside.[10] (See ch. 5 for further discussion of computer crime.)

Other factors that have contributed to renewed interest in information systems security in the 1980s include a growing awareness of the Federal Government's dependence on information technology, and an increasing sense that existing policy in this area is inadequate. For example, a 1982 GAO report said that Circular A-71 has not been implemented effectively because it failed to: 1) provide clear guidance to agencies on minimum safeguards needed, 2) clarify the relationship between measures for national security information and measures for other kinds of information, and 3) provide guidance on telecommunications security.[11]

In part as a result of this renewed interest and controversy over information systems security policies, the executive branch has taken two very significant steps to change these policies. The first was NSDD 145, issued by the President on September 17, 1984, which gives the NSA new authorities and responsibilities for a wide range of military and nonmilitary information security functions. It is to "act as the government focal point for cryptography, telecommunication systems security, and automated systems security." This aspect of NSDD 145 is unusual and worthy of attention—essentially, the directive aims to bring together the separate paths of military and civilian agencies in national security-related information security, and put them both under the guidance of NSA.

NSA's role in this respect will be guided by two interagency committees. One is the the Systems Security Steering Group, a high-level oversight group that meets twice a year. The second is a working group known as the National Telecommunications and Information Systems Security Committee (NTISSC), composed of 22 agency representatives, 12 from the national security community." See table 4-4 for the membership of these committees. NTISSC meets quarterly, and has subcommittees on automated information systems security and telecommunications security that meet more frequently.

The scope of the roles of NSA and NTISSC depends on their interpretation of their mandate to assist in protecting information "the loss of which could adversely affect the national security interest." The extent to which this category includes unclassified information (essentially establishing a fourth level of classification beyond the "top secret," "secret," and "confidential" designations now used) will determine the range of military and civilian agency activities that will be influenced by NSDD 145.

---

[10] See, for example, Joel Zimmerman, "The Human Side of Computer Security," *Computer Security Journal,* summer 1984, pp. 7-19. The relative importance of "outsiders" penetrating information systems is viewed by some as a critical difference between military and civilian information systems. Because personnel running military systems have usually been more carefully "cleared" than those in civil agencies, and because the potential adversaries seeking national security information are much more sophisticated, military computer security experts often emphasize protection from outside penetration. See "Computer Security, The Defense Department, and the Private Sector–A 3-Part Dialogue About Fundamental Objectives and Needs," in the journal referenced above, pp. 53-66. The differences between military and civilian information security needs will be a continuing theme throughout this chapter.

[11] U.S. General Accounting Office, *Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices, MASAD-82-18,* Apr. 21, 1982.

[12] The extent to which NTISSC is "dominated by the military" became an issue in hearings held by the House Science and Technology Subcommittee on Transportation, Aviation, and Materials, June 27, 1985. The U.S. General Accounting Office, in its testimony, indicated that 10 of the 22 representatives are from defense agencies (the Secretary of Defense; the Joint Chiefs of Staff; the Army, Navy, Air Force, and Marine Corps; the Defense Intelligence Agency; the National Security Agency; the National Communications System; and the Assistant Secretary of Defense for Command, Control, Communications and Intelligence). Perhaps more important than the number of defense agency representatives is the number of representatives whose primary concern is the protection of classified information, since the needs and motivations of such representatives are significantly different *from those* of other agencies. Under this criteria it would make sense to add the Director of Central Intelligence, and the Assistant to the President for National Security Affairs, making 12 of 22 committee members from the "national security community," considered broadly.

Table 4-4.—Committees Guiding the Implementation of NSDD 145

Systems Security Steering Group:

1. Secretary of State
2. Secretary of the Treasury
3. Secretary of Defense[a]
4. Attorney General
5. Director of OMB
6. Director of Central Intelligence[a]
7. Assistant to the President for National Security Affairs, chair[a]

National Telecommunlcations and Information Systems Security Committee:

Consists of a voting representative of each of the above, plus a representative designated by each of the following:

8. Secretary of Commerce
9. Secretary of Transportation
10. Secretary of Energy
11. Chairman, Joint Chiefs of Staff[a]
12. Administrator, GSA
13. Director, FBI
14. Director, Federal Emergency Management Agency
15. Chief of Staff, Army[a]
16. Chief of Naval Operations[a]
17. Chief of Staff, Air Force[a]
18. Commandant, Marine Corps[a]
19. Director, Defense Intelligence Agency[a]
20. Director, National Security Agency[a]
21. Manager, National Communications System[a]
22. Assistant Secretarv of Defense for Command. Control, Communications and Intelligence, chai~

[a]Denotes a representative closely associated with the defense/national security community. See footnote 12, in text

SOURCE" National Security Decision Directive 145, unclassified version, "National Policy on Telecommunications and Automated Information System Security, " issued by the President, Sept 17, 1984

The directive is still early in its implementation. NTISSC and its related subcommittees have begun to meet (on a classified basis) to work out the implementation of the directive. They have developed a report on the status of computer and telecommunications security in the government, again classified, although OTA obtained an unclassified extract, discussed below. Some of the other early activities of the NTISSC and its subcommittees include working on a scheme for categorizing sensitive, but unclassified, information in both the military and civilian agencies. They have also developed an OMB bulletin (No. 85-11) that asks agencies to report information to OMB on information security measures for classified systems. NSDD 145 will be discussed in more detail later in this chapter.

The second major recent policy action on information systems security is a new OMB circular, A-130, "Management of Federal Information Resources, " that supersedes and revises A-71 and three other circulars.[13] The revision attempts to present integrated guidance on Federal Information Resources Management, considered broadly. The new circular does not make major changes to A-71, but rather strengthens and clarifies it in a number of areas:

- It defines security as "both the protection of information while it is within the systems and also the assurance that the systems do exactly what they are supposed to do and nothing more . . . . security of information systems is first and foremost a management issue and only secondly a technical problem of computer security. "
- It emphasizes new vulnerabilities in the government as a result of "smaller and more powerful computer systems and new communications technology and transmission media, together with the greater involvement of end users in managing information resources. "
- It acknowledges the relationship between the former Circular A-71 and Circular A-123, "Internal Control, " by noting that agencies should consider information security an essential part of their internal control reviews.[14]
- It expands and clarifies the definition of "sensitive data" to include "data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, rec-

"The other circulars are A-90 ("Cooperating With State and Local Governments to Coordinate and Improve Information Systems"), A-lo8 ("Responsibilities for the Maintenance of Records About Individuals by Federal Agencies"), and A-121 ("Cost Accounting, Cost Recovery, and Interagency Sharing of Data Processing Facilities").

"In 1983, the Office of Management and Budget revised Circular A-123, which, along with the Federal Managers Financial Integrity Act (Public Law 97-255), requires agency heads to analyze safeguards and audit systems (of all kinds, including those applying to information systems), and report to the President and Congress annually with a plan for correcting any weaknesses. A U.S. General Accounting Office review of the first-year implementation of the Financial Integrity Act said that internal controls related to information systems received inadequate coverage in the reviews, and that some agencies were uncertain of the relationship between A-71 and A-123.

orals about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act. "[15]

- It reasserts the need for agencies to define security needs before procuring or starting formal development of application systems.
- It adapts its requirement for risk analyses for all systems to note that "risk analyses may vary from an informal review of a microcomputer installation to a formal, fully quantified risk analysis of a large scale computer system. "
- It requires agencies to establish a security awareness and training program.
- It briefly acknowledges that the Secretary of Defense has a role in information systems security for systems that process "information the loss of which could adversely affect the national security interest, " and directs DOD to provide technical material and assistance to Federal agencies on information systems security. [16]

[15] 'The definition of sensitive data proposed in the draft circular is quite different from the concept of sensitive data in NSDD 145, which considers data sensitive if it is related to national security; the exact definition for NSDD 145 is yet to be released, as will be discussed later in this chapter.

[16] "NSDD 145 required that the Office of Management and Budget review A-71, Transmittal Memorandum #l, and amend it as appropriate for consistency with the directive. Although Circular A-130 states that it has satisfied this requirement (appendix IV, section 2), it has done so only in a *pro forma* manner. On closer inspection, the wording in the circular actually does very little to clarify the substantial confusion about the relative roles of NTISSC, NSA, NBS, OMB, GSA, and other agencies in the area of information security.

MAJOR FINDINGS

Finding 1

The Federal Government faces fundamentally new levels of risks in information security because of increased use of networks, increased computer literacy, an explosion in microcomputer use and decentralized data processing capabilities, and increased dependency on information technology overall.

This finding provides an important foundation for assessing the importance of information systems security as an issue. These trends are also discussed in several other chapters in this report.

Increased Use of Networks

Computer power is becoming cheaper and more widely distributed and the machines are becoming more sophisticated in their capabilities to share data and communicate with one another. As a result, the use of networks of all kinds, from local area networks linking an office's personal computers to dedicated data networks spanning thousands of miles, is expanding rapidly. In addition, an increasing number of computers are accessible via dial-up connections using ordinary phone lines. While these linkages add to the effectiveness of information technology systems, they also raise new vulnerabilities by allowing possible abuses at a distance, and by increasing opportunities for eavesdropping. '7

Increased Computer Literacy

The simple fact that more people know how to use computers, and that computers are becoming easier to use, means that there are more people both inside and outside the Federal Government who have the skills to use information systems for unintended purposes.

[17] OTA's forthcoming study, "New Communication Technologies: Implications for Privacy and Security, " will discuss these issues further. Also see U.S. General Accounting Office, *Increasing Use of Data Telecommunications Calls for Stronger Protection and Improved Economies*, LCD-81-1, Nov. 12, 1980: and U.S. Congress, Office of Technology Assessment, *Electronic Surveillance and Civil Liberties*, OTA-CIT-29 (Washington, DC: U.S. Government Printing Office, October 1985).

Microcomputers, Workstations, and Decentralized Data Processing

As discussed in chapter 2, the Federal Government is in the midst of an explosion in microcomputer use, from almost none in 1975 to estimates of over 100,000 in 1985. In addition to their use as independent data processors, microcomputers that are used as "intelligent workstations"[18] to exchange data with a larger computer and manipulate it independently raise very significant managerial issues. This decentralization of data-processing capabilities reduces the degree of management control over data and information systems use; it increases the number of people using information systems; and these machines have new security problems of their own. On the other hand, decentralized systems can be more secure in some ways because all data are not vulnerable as they would be in one large system.

In essence, designers and users of largescale computers were just beginning to understand information security needs and implement effective measures when the microcomputer appeared on the scene, destroying the fragile developing consensus about security. Westin and Hoffman[19] describe seven key risks particularly applicable to microcomputers:

1. lack of clear organizational policy identifying sensitive information on office automation systems;
2. failure to provide adequate physical-location security for machines and storage media;
3. failure to have key locks on terminals;
4. weaknesses in password systems governing access to central databases from microcomputers;
5. frequent lack of access logs or journals on office systems of connected microcomputers;
6. absence of methods to record efforts to penetrate security of office-based microcomputer systems; and
7. absence of either security education for end users or auditing of user practices.

Other problems include the generally simplistic (and thus hard to protect) architectures of small computer systems, lack of adequate off-site backup for data in small computers, and reluctance of management to demand security discipline from users of small computers.

Management guidelines need to be developed in each of these areas in order to maintain information security. Only 27 percent (37 out of 139) of agencies responding to OTA's Federal Agency Data Request indicated that they had an explicit information security policy for microcomputers.

NBS has attempted to help agencies develop such policies with a recent publication, *Security of Personal Computer Systems: A Management Guide,* January 1985. Nevertheless, there is likely to be some lag between the rapid increase in microcomputer use and the development and implementation of effective administrative measures. An example of such a lag is the fact that the main GSA retail microcomputer store, Office Technology Plus, does not carry any security-related hardware or software; they refer inquiries to their store near the Pentagon.[20] Security is not yet considered an integral part of the world of most microcomputer vendors and users. This situation points to the need for greatly increased vigilance on the part of information system managers and users.

Increased Dependency on Information Technology

As noted in chapter 2, Federal expenditures for information technology have increased significantly, from $10.4 billion in fiscal year 1983 to an estimated $15.2 billion in fiscal year 1986. In addition to using more information

[18] "The term "intelligent workstation" is used by computing experts to refer to a computer terminal that has substantial stand-alone processing capabilities, as opposed to a "dumb terminal," which can only be used to communicate with a shared larger computer.

[19] Alan Westin and Lance Hoffman, "Privacy and Security Issues in the Use of Personal Information About Clients and Customers on Micro and Personal Computers Used in Office Automation," OTA contractor report, February 1985.

[20] OTA site visit, Office Technology Plus, March 1985; telephone conversation with Ken Jones of OTP, February 1986.

technology for traditionally automated applications (e.g., payroll processing), the government is using information technology in a variety of other areas, including decision support, reporting and dissemination of information, and auditing. Many Federal missions, from social welfare programs to revenue collection to air traffic control, are critically dependent on information technology. This escalating intensity and range of use reinforces the importance of effective safeguards and policies regarding privacy and security. Further, in the next decade there will increasingly be new information technologies-such as voice data input/output, digital telephone networks, optical storage of data, and expert systems—with different security problems.

Together, these trends imply that the whole area of information systems security is in flux and the potential problems are perhaps an order of magnitude greater than they were a decade ago. These new levels of risk, along with the major policy changes in the executive branch, suggest the need for increased congressional attention in this area.

Finding 2

Although there has been some progress in the past 5 to 10 years, there is widespread evidence that Federal policy requiring the use of appropriate information systems security measures has been ineffective.

There is substantial evidence pointing to continuing (and perhaps worsening) information security problems in the Federal Government. The evidence comes principally from five sources–GAO reports, OTA's Federal Agency Data Request, other audits, congressional hearings and studies, and expert opinion.

GAO Reports

Table 4-5 lists some of the GAO reports over the past decade that have been critical of information security practices in Federal agencies. These reports range from audits of specific agencies, such as the Social Security Administration or the Financial Management Service, to broader studies critical of governmentwide practices. GAO's 1982 study, *Federal Information Systems Remain Higly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices,* mentioned earlier, argued that OMB's policy in A-71 was never clear enough, it did not establish minimum standards, and agency performance was not reviewed for compliance.

GAO has conducted a survey of information security practices at key computer installations of 17 Federal agencies. The results, summarized in tables 4-6 and 4-7, show that only

Table 4-5.—Selected GAO Reports Identifying Major Information Systems Security Problems, 1975-85

General:

Computer-Related *Crimes in Federal Programs,* Apr. 27, 1976, FGMSD-76-27.

Fraud in Government Programs: *Ho w* Extensive Is It *and How Can /t Be Controlled?* Sept. 30, 1981, AFMD-81-73.

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

Computers and data processing:

Managers Need *To Provide Better Protection for Federal Automatic Data Processing Facilities,* May 10, 1976, FGMSD-76-40.

Automated Systems Security—federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data, Jan. 23, 1979, LCD-78-123.

Central Agencies Compliance With OMB CircularA-71, Transmittal/ Memorandum No. 1, Apr. 30, 1980, LCD-80-56-I.

Most Federal Agencies Have Done Little Planning for ADP Disasters, Dec. 18, 1980, AFMD-81 -16.

Telecommunications:

Vu/nerabi/ities of Telecommunications Systems to Unauthorized Use, Mar. 31, 1977, LCD-77-102.

Increasing Use of Data Telecommunications Calls for Stronger Protection and /reproved Economies, Nov. 12, 1980, LCD-81-1 .

Audits of specific agencies:

/RS' Security Program Requires Improvements To Protect Confidentiality *of /ncome Tax /formation,* July 11, 1977, GGD-77-44.

Flaws in Controls Over the Supplemental Security Income Computerized System Causes Millions in Erroneous Payments, Aug. 9, 1979, HRD-79-104.

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

Solving Social Security's Computer Problems: Comprehensive Corrective Action Plan and Better Management Needed, Dec. 10, 1981, HRD-82-19.

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

/improvements Needed in. Genera/ Automated Data Processing Controls at the National Finance Center, July 12, 1985, AFMD-85-38.

SOURCE Office of Technology Assessment

Table 46.—Systems Meeting GAO Criteria for Physical, Technical, and Administrative Security Safeguards

	Number of systems having safeguards
Physical safeguards:	
Physical perimeter.	16
Entry by badge or cypher lock	24
Use of security guards	22
Use of smoke and/or heat detectors	24
Technical safeguards:	
Identification and authentication	23
Audit trails or logs	10
Discretionary access controls (authorization).	24
Administrative safeguards:	
Separation of duties ... , ...	15
Physical, administrative, and technical procedures tested	20
Audit trail information reviewed	10
Passwords required to be changed	21
Have all safeguards.	5[a]

[a]Although these systems contained all evaluated safeguards, they may still be vulnerable because: 1) GAO evaluated selected safeguards only, and 2) all evaluated management responsibilities were not implemented GAO does not know how vulnerable the systems may be because this survey did not involve testing the effect iveness of the safeguards.
NOTE Total number of systems examined = 25

SOURCE: Statement of William Franklin, Associate Director, IMTEC Division, General Accounting Office, before the House Committee on Science and Technology, Subcommittee on Transportation, Aviation, and Materials, "Automated Information Systems Security in Federal Civil Agencies," Oct 29, 1985.

Table 4-7.—Systems Meeting GAO Criteria for Computer Security Management Evaluation

Management responsibilities	Number of systems meeting requirements
Risk management	8
Training	2
ADP personnel security	2
Assigned responsibility	4
Budgeting and accounting for security cost.	1
Contingency plans (exist and tested).	9
Independent evacuation or audit	19
Written procedures	11

NOTE: Total number of systems examined =25

SOURCE: Statement of William Franklin, Associate Director, IMTEC Division, General Accounting Office, before the House Committee on Science and Technology, Subcommittee on Transportation, Aviation, and Materials, "Automated Information Systems Security in Federal Civil Agencies," Oct. 29, 1985

5 of these 25 critical systems had all appropriate safeguards. Two areas in which a majority of systems fell short were:

1. the use of audit logs to monitor system activity; and
2. management responsibilities, including provisions for effective training, personnel security, assignment of responsibilities, budgeting and accounting for security cost, proper contingency plans, and available written security procedures.

OTA's Federal Agency Data Request

Table 4-8 shows the percentage of Federal agency components that reported using a variety of information security techniques for sensitive, unclassified information. Only 34 percent of agencies reported that they have screened all of their sensitive, unclassified computer applications for sensitivity and appropriate safeguards before use, and only 61 percent report using personnel screening for all of these applications. Both of these measures are mandated by A-71/TM-1, and by the new circular, A-130. In addition, only 78 of 134 (58 percent) agencies reported that they had conducted one or more risk analyses in the last 5 years, a procedure also mandated by OMB's guidance. Finally, only 57 percent of agencies reported that they had (or were in the process of developing) contingency plans to handle the disruption of their major mainframe computers. The agencies did report significant use of passwords, backup of key data files, and physical security for hardware, although only 58 percent reported that they used audit software to monitor the activities on systems processing sensitive, unclassified information.

Other Audits

Reports by the agencies' own inspectors general, and by the agencies' upper management under the Federal Managers Financial Integrity Act, also frequently identify weaknesses—many of them long-standing-in control procedures related to information security. See table 4-9 for examples. A GAO review of agencies' internal control reports submitted under the Federal Managers Financial Integrity Act indicated that the number of agencies reporting material weaknesses in automatic data processing controls rose from 10 in 1983 to 14 in 1984 (out of a total of 18 of the largest agencies) .21 In addition, the Na-

"U.S. General Accounting Office, *Financial Integrity Act: The Government Faces Serious Internal Control and Accounting Systems Problems.* December 1985.

Table 4-8.—Security Techniques in Use by Federal Agencies in Unclassified But Sensitive Applications

Technique	Number of components using	Percent	Number reporting use for 1000/0 of systems	Percent
Applications screening	67	48.20/o	47	33.80/o
Personnel screening	102	73.4	85	61.2
Audit software	80	57.6	30	21.6
Restrictions on dial-up access	85	61.2	65	46.8
Password controls	133	95.7	106	76.3
Encryption	30	21.6	9	6.5
Backup hardware	87	62.6	48	34.5
Backup of key data files	133	95.7	110	79.1
Physical security for hardware	127	91.4	94	67.6
Other	9	6.5	5	3.6

NOTE Total agency components responding 139

SOURCE OTA Federal Agency Data Request

Table 4-9.—Examples of Other Audits Identifying Significant Information Security Problems in Federal Agencies

Department of Energy, Inspector General, "Screening Contractor Employees Having Access to Sensitive, Unclassified Data Contained in Departmental Computer Systems," Oct. 20, 1981, MR 81-44.

General Services Administration, Inspector General, "insufficient Controls and Policies Exist To Effectively Procure, Manage, and Use Microcomputer Assets," Region 10, undated, A40349/101F1840926.

Agency for International Development, Auditor General, "Survey of Computer Security for AID's Washington Based Automated Information System, " Dec. 24, 1980, 81-26.

Department of the Interior, Inspector General, "Synopsis of Recent ADP Audit Findings, " February 1985, H-MO-MOA-06-85(a).

Agencies listing ADP security flaws in their reports under the Federal Managers Financial Integrity Act:

Department of Education
Department of Commerce
Nuclear Regulatory Commission
Department of Health and Human Services-Health Care Financing Administration, Public Health Service
General Services Administration
Department of Agriculture
Department of Housing and Urban Development
Department of the Treasury
Office of Personnel Management
Department of Labor
Veterans Administration
Small Business Administration
National Aeronautics and Space Administration
Environmental Protection Agency
Department of State
White House
Department of Defense

SOURCE Off Ice of Technology Assessment. various agency reports

tional Telecommunications and Information Administration, as part of its duties under PD-24, discussed earlier, performed 28 surveys of telecommunications and information vulnerability in civilian agencies during 1979 to 1984, involving interviews and briefings with hundreds of agency staff. A summary of the findings from the first 21 surveys is presented in appendix 4B at the end of this chapter, and indicates significant problems in the area of telecommunication security in particular.

Finally, the first annual report from the NTISSC (mandated by NSDD 145) describes the government posture in information systems security as "poor and rapidly getting worse, and in communications security as "unsatisfactory. The report recommends, in part, that the government develop a coherent framework for computer security policies, and that such policies require each system processing classified or sensitive data to have a personal identification and authentication system, audit trails that keep a record of activity, a designated security officer, a written security plan, control over physical access, and security controls on removable storage media. The report also calls for cabinet-level action to increase manpower and funding in computer and communications security governmentwide.[22]

See chapter 5 for further studies of computer crime in the Federal Government.

Congressional Studies and Hearings

Several congressional committees have played. a key role in evaluating the state of informa-

[22] "National Telecommunications and Information Systems Security Committee, "First Annual Evaluation of the Status of Telecommunications and Automated Information Systems Security in the United States Government, " Aug. 10, 1985 (unclassified extract).

tion security in the Federal Government. Two reports in the mid- 1970s by the Senate Committee on Government Operations (now Governmental Affairs), then chaired by Senator Abraham Ribicoff, noted widespread computer security problems and urged improved coordination in policy regarding computer security and abuse.[23] A 1983 report from the same committee, now chaired by Senator William Roth, also highlighted some of the same issues and concerns.[24]

On the House side, the Committee on Science and Technology, Subcommittee on Transportation, Aviation, and Materials, formerly chaired by Representative Dan Glickman, has held a series of hearings on computer and telecommunications security, and has issued a report urging more leadership in security policy, more Federal research and development and educational programs in computer security, and the establishment of a national commission on information security and policy issues.[26] The House Committee on Government Operations has also held hearings, particularly on the role of NSA and NSDD 145.[26]

Expert Opinion

Based on OTA's workshops and other contacts with Federal information technology managers, most information security officials agree that there are serious, continuing security problems. While many officials would assert that there has been some improvement in the past few years as Federal personnel have become more aware of security issues (mostly through publicity about hackers), they would also acknowledge that frequently there is a lack of attention to information security on the civilian side of government. OMB staff, for their part, openly acknowledge that A-71/TM-1 has not been effective, and this realization is one of the motivations for revising that circular and incorporating it into the new circular on Federal information resources management.

Finding 3

Three key factors inhibit appropriate Federal information security measures:

1. competition for resources in Federal programs, which tends to limit spending for a "latent" issue like security;
2. a lack of awareness or motivation among agency personnel; and
3. an absence of clear guidance on appropriate security measures.

While there are many and varied reasons for the lack of attention paid to information security among Federal programs, these three factors seem to be common themes mentioned frequently in conferences, personal contacts, and workshops with Federal agency staff .27

'Senate Committee on Government Operations, *Problems Associated With Computer Technology in Federal Programs and Private Industry: Computer Abuses,* 94th Cong., 2d sess., 1976; and *Computer Security in Federal Programs,* 95th Cong., 1st sess., 1977.

"Senate Committee on Governmental Affairs, Permanent Subcommittee on Investigations, *Federal Computer Security: An Analysis of Congressional Initiatives and Executive Branch Responsibilities* (prepared by the Congressional Research Service), 98th Cong., 1st sess., 1983.

'House Committee on Science and Technology, Subcommittee on Transportation, Aviation, and Materials, hearings on "Computer and Communications Security and Privacy, " Sept. 26, Oct. 17, and Oct. 24, 1983, and Sept. 24, 1984; and report, *Computer and Communications Security and Privacy,* April 1984. The Subcommittee has also held hearings evaluating National Security Decision Directive 145, June 27, 1985. These will be discussed in more detail later in the chapter. Finally, both the House and Senate have held hearings on the vulnerability of Federal information technology to computer crime. These will be discussed in more detail in ch. 5.

"'See Jim Dray and Fred Wood, OTA, Statement for the Record Before the House Government Operations Subcommittee on Legislation and National Security Hearing on H.R. 2889: The Computer Security Research and Training Act of 1985, Sept. 18, 1985.

See, for example, GAO and other audit reports referenced above; also John O'Mm-a, "Computer Security: A Management Blindspot, " *Computer Security Handbook* (Northborough, MA: Computer Security Institute, 1984), pp. 2A1-2A4; Joel Zimmerman, "The Human Side of Computer Security, " *Computer Security Journal,* summer 1984, pp. 7-19.

These factors are most applicable to civilian agencies (and, in many cases, to the private sector as well). In sensitive defense or national security applications where the threats are more apparent (e.g., foreign adversaries), awareness and willingness to spend money for security are likely to be much higher. And, as noted earlier in the chapter, the defense and intelligence agencies have a great deal of expertise in security, and particularly detailed guidance for their staff on appropriate measures for protecting information systems. However, prob-

Competition for Resources

Security measures frequently cost money, and they almost always exact a "tax" on the productivity of information systems. Audit trails that record the activities on a system, for example, require computer time and resources, and they take time and expertise to review. If passwords are required to be more than six characters and changed every 3 months, they are often harder to remember.[28] The *use* of encryption systems requires time to encrypt and decrypt, time and staff to manage the encoding keys, etc. If given a choice between spending resources on security measures, or spending those resources on features or staff to enhance the performance of an information system, most managers would choose the latter, especially in a climate of tight budgets.

Further, security expenditures are hard to identify and review because security has not usually been included as a separate line item in agency budgets or procurements, and the number of staff hired to handle information security exclusively is usually very small and of relatively low status within the agency. Table 4-10 shows the funding and number of full-time equivalent staff that agencies reported to OTA for computer and communications security. The reported figures are extraordinarily varied, and they probably do not include the full range of information security activities, since (as GAO noted in its study of 25 key systems) agencies tend to be unprepared to account for security costs, and many staff handle information security part-time. However, the total dollar figure reported by all agencies responding ($33.5 million in fiscal year 1985) would seem low compared to OMB's estimate that the government spent $13.9 billion for information technology in fiscal year 1985. Clearly, though, more authoritative numbers than these brief responses to OTA's Federal Agency Data Request are needed as a base for policy action.

OMB's rationale for not segregating security expenditures in budget requests is that security is primarily a component of good information systems management. "It would be a mistake to divide out computer security from computer management. They should be intertwined. '[29] Computer systems designers agree that the most productive way to seek out security in information systems is to incorporate security concerns throughout the system's design, implementation, and management. But the net result of OMB policy might be that, in some cases, system designers do not build in security because they believe it will compete with the funds available for hardware and software that increase performance. As an OMB official noted:

> I would also say that the annual budget process–and I depart a little bit, if I may, from my position as Deputy Director of Office of Management and Budget–tends to emphasize reduced funds rather than increasing expenditures for enhanced telecommunication and data processing and security .30

The implementation of NSDD 145 is likely to change the way agencies budget for information security, although the exact nature of those changes has not yet been determined. The directive provides that the Director of NSA shall:

- review and assess annually the *telecommunications* system security programs and budgets of the departments and agencies of the government, and recommend alter-

---

lems in awareness, willingness to spend funds, and clarity of guidance are also significant for some defense applications, particularly those that deal with unclassified information. (OTA, personal communications with Defense Logistics Agency staff, Jan. 22, 1985).

'"Computer security experts would argue that a well-designed, secure system-one for which security has been designed in from the start and not added later-can run just as efficiently as an insecure one, and in some cases better. In addition, NSA has had some success in using longer passwords composed of real words, such as ''ma pa sam, which are more secure than a short password but not as hard to remember as a series of unrelated characters, such as " lxgh7ytrb. " (Sheila Brand, National Computer Security Center, personal communication, September 1985).

"'Joseph Wright, Deputy Director, Office *of* Management and Budget, testimony to the House Science and Technology Subcommittee on Transportation, Aviation, and Materials hearings on "Computer and Communications Security and Privacj', Sept. 24, 1984, p. 5.

"'Ibid., p. 4.

Table 4-10.—Federal Agency Expenditures and Staffing for Computer and Communications Security

Agency	Funding (in thousands)			Number FTE[a]		
	1980	1983	1985	1980	1983	1985
Department of Agriculture	**$2,295**	$5,516	**$11,866**	6.4	17.6	33.0
Department of Commerce	**2,565**	2,601	**2,649**	21.0	21.5	22.0
Department of Defense	**762**	2,900	**6,257**	35.0	82.5	133.5
Department of Education	**0**	280	**330**	·	5.0	5.75
Department of Energy	**0**	263	**170**	1.0	0.5	0.5
Department of Health and Human Services	521	486	473	10,25	10.25	13.0
Department of Housing and Urban Development	0	90,000	0	1.0	1.0	1.0
Department of the Interior	132	249	**297**	2.0	8.0	**9.5**
Department of Justice	80	234	**287**	2.0	113.4	**134.0**
Department of Labor	40	80	**120**	1.0	2.0	**3.75**
Department of State	0	520	598	1.0	5.0	**8.0**
Department of Transportation	46	96	932	10.3	11.3	**13.5**
Department of the Treasury	164	527	1,607	48.8	14.6	**29.4**
Subtotal, cabinet agencies	$6,605	$13,842	$25,585	140.0	293.0	407.0
20 selected independent agencies (total)	749	2,362	7,927	62.0	64.0	72.0
Total	$7,354	$16,204	$33,511	202.0	357.0	479.0

[a]FTE = Full-time equivalent staff members.
NOTE: Some figures are rounded,
SOURCE: OTA Federal Agency Data Request

natives, where appropriate, for the executive agent and the steering group; and
- review annually the aggregated automated *information systems* security program and budget recommendations of the departments and agencies of the U.S. Government for the executive agent and the steering group.[31]

It is not yet clear what kind of authority NSDD 145 confers on NSA and the steering group. One key NSA official said in congressional testimony that while agencies retained autonomy on *whether* to implement security measures, NSA would control what would be implemented:

> Once a department or agency head has chosen to spend money on telecommunications security or automated information systems security, the NSA, as National Manager, prescribes or approves which COMSEC [communications security] or COMPUSEC [computer security] technique, system or equipment will be used.[32]

Finding 4 will discuss NSDD 145 in more detail.

[31]Sections 7j-k of the directive (emphasis added). See table 4-4 for the composition of the Systems Security Steering Group.
[32]Walter G. Deeley, (former) Deputy Director, Communications Security, NSA, statement to House Science and Technology Subcommittee on Transportation, Aviation, and Materials, June 27, 1985.

Lack of Awareness and Motivation

Another common theme in many of the audit reports cited above is that frequently top agency staff and many general users are unaware of the need for information security. Thus, security staff commonly report that, for example, computer users will write down their password on the wall next to their terminal.[33] This lack of awareness is particularly acute among microcomputer users, most of whom are new to the special security problems raised by the use of their machines. Some of the factors that increase the awareness of computer users toward security needs include press attention, top-level management support, and education and training programs. A later section of this chapter will discuss these in more detail.

Lack of Clear Guidance

Even when agencies are aware of security risks, it is often unclear what measures are appropriate. In short, the current policy guidelines are not clear and specific enough to give Federal managers a concrete idea of what they should do to implement the policies. Circulars A-71 and A-130 do not provide guidance on

[33]See, e.g., Zimmerman, op. cit.

security measures appropriate for different applications; rather they mandate a risk analysis to help make this assessment. However, agencies have reported increasing frustration with risk analyses. They have frequently been complex, expensive, and oriented toward physical or technical security measures for large-scale computing centers, at the expense of simpler, cheaper, common-sense strategies.[34]

Federal Government policy and security experts have responded to this problem in several ways. First, substantial efforts are under way to make risk analysis techniques simpler, cheaper, and more helpful.[35] Second, there has been some substantial movement toward developing a set of minimum security standards for various information system applications. Such standards represent a promising technique because they make appropriate actions clear, and eliminate the need for formal risk analyses except in unusual or particularly sensitive situations. As noted earlier, USGS, for example, has reported success in using a technique based on a simple questionnaire that asks system managers to determine the degree of sensitivity of their applications, and to indicate whether they have implemented a set of minimum security measures.

The National Computer Security Center (NCSC)[36] and the NTISSC (the implementing committee for NSDD 145) are also working on a variety of schemes to categorize the sensitivity of unclassified national security-related information and, ultimately, to specify appropriate security measures for each level of sensitivity. In related work, the NCSC has already developed a scheme for categorizing the technical security features of computer systems, ranging from those that require little more than password control (the "Cl" level) to those whose operating systems can pass sophisticated tests of design integrity (the "Al" level). The center has an ongoing program for evaluating products submitted by vendors in order to rank them according to their technical security-related features.[37] Each of these categorization schemes is potentially a very important step in helping to make the choice of information security measures for Federal systems clear and explicit. -

Finding 4

As NSDD 145 is implemented, it becomes increasingly clear that NSA and the committees guiding implementation of the directive will play a significant if not dominant role in all aspects of information security in the Federal Government whether or not the information is classified. NSDD 145 is likely to result in stronger governmentwide leadership in information security policy; however, concerns have been expressed that it puts the national security community in an unusual, influential if not controlling position on a key aspect of the Nation's information policy.

While the language of NSDD 145 focuses on national security-sensitive information and hostile threats, it also states that NSA is to act as the government's focal point for information security, and

> . . . review and approve all [presumably national security-related] standards, techniques, systems and equipments for telecommunications and automated equipment security.

The implementation of NSDD 145 is still in progress, and NTISSC is in the midst of defining sensitive national security-related information and thus the scope of their jurisdiction. However, early indications from participants on NTISSC, as well as congressional testimony by NSA officials, are that the committee may intend to construe their jurisdiction very broadly, to include, for example, information that is sensitive for reasons of privacy,

---

'"See, for example, Robert Campbell, "Agency Risk Analysis Still Inadequate, " Mar. 29, 1985, p. 23; and *'OMB Directive Is Dramatically Out-of-Date, " *Government Computer News,* May 10, 1985, p. 31.

"See, for example, the proceedings from the Air Force's first conference on risk analysis techniques, Jan. 21-23, 1985, Montgomery, AL,

"The DOD Computer Security Center (under the auspices of NSA) changed its name to the National Computer Security Center in fall 1985.

[37] Department of Defense Computer Security Center. *Department of Defense Trusted Computer System Evaluation Criteria, CSC-STD-O01-83,* August 1983. This is also known as "The Orange Book. "

commercial competition, or agency decision-making.[38]

The only other significant technical resource in the government for information security is the NBS Institute for Computer Sciences and Technology (ICST). ICST has approximately nine full-time equivalent staff devoted to information security in the government as a whole (including some working on defense-related security). The National Computer Security Center has more than 200.[39] Thus the de facto assumption behind NSDD 145 is that NCSC can effectively serve as a standards-setter and technical resource for all (or almost all) Federal agency needs for security.

This approach is controversial, with major advantages and disadvantages. Earlier findings in this chapter have documented the need for clear and useful policy action in information security, and the mechanism set forth in NSDD 145 could provide the leadership and visibility to facilitate that action. NCSC can build on a great wealth of expertise in information security matters. In addition, NTISSC provides a significant opportunity for civilian agencies to help guide the process, and it provides an important forum for agencies to share security problems and solutions with each other.

Yet, the same centralization of authority that facilitates leadership and effective action also places NSA (as national manager for computer security) and the Secretary of Defense (as executive agent) in an unusual controlling position on security policy for both military and civilian agencies. This situation has led to heated debate in a 1985 congressional hearing. Representative Jack Brooks, for example, called the directive:

> . . . one of the most ill-advised and potentially troublesome directives ever issued by a President. . . .
>
> First, it was drafted in a manner which usurps Congress's role in setting national policy. . . .
>
> Second, the directive is in conflict with existing statutes which assign to the Office of Management and Budget, the Department of Commerce, and the General Services Administration the sole responsibility for establishing government-wide standards, guidelines and policies for computer and telecommunications security. . . .
>
> Finally, I seriously question the wisdom of the President's decision to give DOD the power to classify, hence control, information located in the civilian agencies and even the private sector which, in DOD's opinion, may affect national security .40

In addition, the extent to which the needs of the civilian side of the government and the private sector mesh well with the needs of the national security sector is open to serious question. Some have asserted that these needs are quite different. For example, before the founding of the Computer Security Center in 1982 some experts argued that the government's primary resource on information security issues should be independent of DOD and NSA.[41] Many of the original arguments against centering the technical resources at NSA concerned the possibility of excessive secrecy. Another disadvantage has recently been argued; namely, that there are important differences between the needs of the national security sector on the one hand, and of the other agencies and the private sector on the other. This disagreement has simmered for several years. In 1984, the *Computer Security Journal* published a "dialogue" between the director of NSA and a prominent private sector

[38] A NSA/NTISSC staff member indicated in early 1986 that the NTISSC was leaning toward a definition of "sensitive for national security reasons" that would leave the final judgments in the hands of the agency holding that information. NTISSC would provide criteria to help agencies make such a judgment. This proposal is still in draft form, however.

[39] OTA's interviews with Robert Brotzman, National Computer Security Center, December 1984, and Dennis Branstad/Stuart Katzke, NBS, February 1985. It should also be noted that for several years in a row, the Administration has proposed to eliminate or severely cut the budget of the Institute for Computer Sciences and Technology, which runs the information security and Federal Information Processing Standards programs at NBS.

[40] Representative Jack Brooks, statement before the Subcommittee on Transportation, Aviation, and Materials, House Committee on Science and Technology, June 27, 1985.

[41] Willis Ware, Rand Corp., personal communication, February 1985.

computer security consultant. As the journal's editors summarized:

> The DOD position is clearly stated: prevention of unauthorized access is the primary need. Others in the private sector, however, contend that far greater attention must be paid to the potential for system misuse by persons who already possess authorization.
>
> Unfortunately, this difference of outlook is more than an academic disagreement of two parties with fundamentally different needs. NSA has begun actively promoting the idea that its primary need for multilevel access security (unquestionably a real need for national security areas) is shared to a large extent by the private sector. NSA does this openly, with the objective of lowering its own costs by creating a sufficiently large market base to bring about economies of scale. There is a significant concern that this will divert resources away from the real problems of most private sector organizations-and, indeed, of most government agencies as well.[42]

Some observers have noted that the Computer Security Center's position emphasizing outside penetration may be changing, and that it may change further as NSDD 145 is implemented.[43] However, serious differences remain between national security and civilian needs. These tend to occur especially in the marginal zones of security, e.g., applications that process unclassified sensitive data, but do not need and cannot afford NSA-style security measures. Although the NCSC staff say they intend to change and develop more expertise in simpler, cheaper measures[44] the extent to which they will be successful in bridging the traditional gap between their techniques and those outside of the national security community remains to be seen.

Another difficulty with the new NSDD 145 arrangement for some civilian agencies is the secrecy of the procedures involved. Though in fact many of NCSC's activities are open in a way unusual for NSA,[46] NTISSC and related committees guiding the implementation of NSDD 145 require top secret and "SI/TK" special clearances. This prevents many stakeholders from knowing about or influencing the implementation of NSDD 145, and was one of the reasons cited for the previous directive, PD-24, not being as successful as intended.[46] Clearance procedures have also prevented at least one set of civilian agency representatives to one of the NTISSC subcommittees from participating in the first few months of activity because the required clearances had not been obtained.[47] And despite the fact that NTISSC aims to have a broad representation from civilian agencies, several of the largest agencies are not participants, including the Departments of Health and Human Services, Housing and Urban Development, and the Interior. Presumably these agencies were excluded because they have little national security-related data, although they do have data that are sensitive for privacy, agency operations, or proprietary reasons.

The new role of NSA as a result of NSDD 145 is a sensitive subject for other reasons as well. Because of the dominance of the national security agencies in the information security arena, it may be difficult for other individuals and organizations (including consultants or other government officials who work closely with NCSC) to frankly and openly present their views on NSDD 145.[48]

Finding 5

> Possible actions to improve Federal information systems security include: more intensive congressional oversight, changing budget procedures with information security receiving higher priority and visibility, designating a ci-

---

"''Computer Security, the Defense Department, and the Private Sector-A 3-Part Dialogue About Fundamental Objectives and Needs," *Computer Security Journal,* summer 1984, pp. 53-66.

"OTA interviews, Dennis Branstad and Stuart Katzke, NBS, February 1985.

"Computer Security Center briefing for Federal agencies on the implementation of NSDD 145, Mar. 15, 1985, Institute for Defense Analyses, Alexandria, VA.

[45] See Sherizen, op. cit.

"Clearly, there are reasons for specific information security data to be classified, especially when it could lead a potential adversary to weak points in an agency,

[47] OTA interview with GSA staff, March 1985.

[48] Based on discussions with several key consultants and stakeholders.

vilian agency to be responsible for security training and technical support in the nonmilitary sector, and revising and clarifying NSDD 145.

More Intensive Congressional Oversight

Congress has played a very useful role in deliberations on information security policy, as noted in earlier sections of this chapter. Congressional hearings are a key forum in which broad issues regarding computer and telecommunications security can be openly raised. On the other hand, the management of information security in Federal agencies is intimately linked to many other aspects of agency management, and many Federal officials express the fear that Congress will usurp their management prerogatives if it attempts to determine security policies within agencies.

While it would clearly be unwieldy for Congress to attempt to directly manage information security in individual agencies, there is just as clearly a role for congressional oversight and policymaking in this area. Some of the key aspects of this issue that Congress is well-suited to examine include the balance between military and civilian interests in developing security policy, the usefulness of new programs to facilitate good security practices, and the relation of information security to privacy and other civil liberties.

Congressional hearings focused on the increasing importance of information security, such as those held by the House Committee on Science and Technology, Subcommittee on Transportation, Aviation, and Materials, help Congress become better informed on the topic. In addition, the various oversight committees in both Houses may wish to include information security as a regular component of their agency oversight hearings, particularly during the implementation of major computer-related programs in agencies. Congress could hold hearings on the willingness of information system vendors to build appropriate security measures into their products. One security expert speculated that the visibility of congressional hearings might be the most effective way to motivate vendors to build in such security, just as car manufacturers routinely include safety features such as seatbelts.[49]

Congress could also maintain close congressional oversight of the implementation of NSDD 145. Possible topics for oversight include the roles of the military and civilian agencies concerning protection of sensitive, unclassified information; the scope and degree of control NTISSC and NSA exert; the effectiveness of the new policy in promoting better information security; and the relation of NSDD 145 to OMB's Circular A-130.

Revised Information Security Budget Procedures

The budget procedures could be changed to provide more visibility for computer and telecommunications security in agency budget requests. Agencies usually do not break out their expenditures for information security, making oversight and cross-agency comparisons difficult. Agencies could specify their expenditures for security (both for staff and as components of information system operating expenses) and/or OMB could conduct a special analysis on this topic. The intent of this would be to make oversight of information security easier; a possible drawback is the additional paperwork that it would generate for the agencies or OMB. OMB and/or GA0[60] could first study in more depth the implications of such a change in budgeting procedures. As an alternative, Congress and/or OMB could request and examine the information security budgets that agencies will be submitting to NTISSC, and could examine closely the portions of agencies' annual internal control reports (submitted under the Federal Managers Financial Integrity Act of 1982) that relate to information security.

"OTA interview with Robert Courtney, Jr., July 1985.

"GAO'S recent survey of 25 key Federal computer systems noted that agencies tend to be unable to account for security costs, and argued that lack of such accounting can lead to "uncontrolled overprotection, failure to identify inadequate controls, resource conflicts leading to inadequate safeguards, inability to monitor cost-effectiveness of controls, compare costs, monitor plans, etc. " (Statement of William S. Franklin, GAO, before the Subcommittee on Transportation, Aviation, and Materials, app. III, Oct. 29, 1985, pp. 14.)

Designate Civilian Agency for Information Security Training

An existing civilian agency could be designated to provide training and support for computer and telecommunications security in the civilian sector of government. Representative Dan Glickman has proposed a bill, entitled the Computer Security Research and Training Act of 1985 (H.R. 2889), which would formally designate NBS as a lead agency to do background research and establish guidelines for agencies' security training. In addition to the formal designation, the legislation could provide additional operating funds for NBS in this area. Such a measure could strengthen the technical resources on information security on the civilian side of government, help ensure that nonmilitary security needs are met, and reduce the likelihood that NCSC will have a monopoly on computer security policy and practices. On the other hand, this could result in some duplication of effort (although not necessarily undesirable) between the civilian and military sectors.

The Administration has argued that H.R. 2889 is unnecessary because NBS already has an implied mandate to conduct information security research through the Brooks Act of 1965. They also point out that NBS and NSA work together well and coordinate their activities in information security. While both of these points are essentially correct, H.R. 2889 would strengthen and clarify the role of NBS in the new security policy framework of NSDD 145.

Of course, funds for NBS's work in information security could be increased without formally changing the status or designation of NBS in this area.

Revise or Clarify NSDD 145

Congress could codify part or all of NSDD 145 into-law, clarifying the roles of NSA, GSA, OMB, NBS, and others in the process. Such an effort should include examining the roles of the central agencies in developing information security policy. To some extent, NSDD 145 contradicts congressional mandates giving OMB and GSA authority to set policy regarding information technology. Codification could help establish a proper congressional role in development of information security policy; on the other hand, a congressionally developed and monitored statute may be less flexible than a Presidential directive, and might hinder the effective implementation of NSDD 145.

Congress or the executive branch could rework the structure and intent of NSDD 145. The degree to which it is appropriate to change NSDD 145 is largely dependent on how much Congress objects to placing NSA and DOD in charge of this aspect of national information policy. NSA and DOD have been, and will likely continue to be, very significant players in information security. In fact, NTISSC itself seems to be a very useful device for agencies to coordinate policy and share ideas on information security. However, by codifying NSDD 145 Congress could remove those aspects of NSDD 145 that give NSA and NTISSC approval authority over civilian agencies' budgets and determinations of information sensitivity. In such a codification, Congress could also develop its own definition of sensitive information that would determine in a general sense the kinds of information agencies should protect. Such an action would diffuse some of the authority of NSA and NTISSC, and thus could dilute some of the potential leadership these groups could assert to improve information security. This option implicitly accepts some dilution of effectiveness in return for a lesser degree of military/national security control over information systems security policy.

The version of H.R. 2889 as amended by the House Committee on Government Operations essentially reworks NSDD 145, giving NBS primary authority for computer security research and training programs for systems that are not used for critical military or intelligence applications.[51] The advantage to defining the

[51] "Specifically, H.R. 2889 limits NBS's authority to those systems that are covered by the Brooks Act or Paperwork Reduction Act. The wording of those acts explicitly excludes juris-

(continued on next page)

NBS role this way is that there is a much cleaner distinction between the roles of NBS and NSA than there is between information "the loss of which could adversely affect the national security interest" and other information. Thus, such a definition could also help to alleviate concerns about placing the national security community in a controlling position over unclassified civilian information policy. On the other hand, this might work against one of the key purposes of NSDD 145, namely, the desire to improve security of information that was not classified but still critical to the national interest.

(continued from previous page)

diction over information technology that: 1) involves intelligence activities; 2) involves cryptologic activities related to national security; 3) involves the direct command and control of military forces; 4) involves equipment which is an integral part of a weapon or weapons system; or 5) is critical to the direct fulfillment of military or intelligence missions, provided that this exclusion shall not include automatic data processing or telecommunications equipment used for routine administrative and business applications such as payroll, finance, logistics, and personnel management (44 U.S.C. 3502).

APPENDIX 4A.–HIGHLIGHTS OF INFORMATION SECURITY POLICIES OF SELECTED AGENCIES

Department of Agriculture: "ADP Security Manual," DM3140-1, July 19, 1984:

–Separates Automatic Data Processing (ADP) facilities into Type I (large, multi-agency, general purpose facilities), Type II (general purpose computers serving multiple users concurrently), and Type 111 (other data and word processing equipment).
–Designates application systems as sensitive if compromise could result in fraud or illegal gains, failure to produce time-critical data, violation of national defense disclosure requirements, unauthorized disclosure of private or proprietary data, adverse effect on ongoing investigations or agency operations, or adverse effect in life-threatening situations.
–Requires adequate physical security, designated security officers, annual security reviews, security plans, and backup and contingency plans for critical systems. Facility managers may determine the need for software access controls, data and software protection, and audit trails.

Department of the Treasury: "Information Systems Security," Directives Manual chapter TD 81, Section 40, April 2, 1985:

–information processed, stored, or communicated by information systems will be placed in three basic categories: national security, sensitive, and public information.
—Sensitive information includes delicate, sensitive, regulatory, financial, law enforcement, privacy, life and mission critical, and proprietary information as well as Officially Limited Information.
–Unauthorized disclosure or manipulation of sensitive information could cause damage such as loss of life or personal injury, loss of property through fraud or theft, loss of privacy, impairment of enforcement or regulatory functions, unfair personal or commercial advantages, or damage to businesses' proprietary secrets.

Department of the Treasury: "Electronic Funds and Securities Transfer Policy, " Directives Manual chapter TD 81, Section 80, August 16, 1984:

–Requires the use of the Data Encryption Standard to authenticate electronic funds transactions by the Federal Government. All Federal EFT systems shall be in compliance by June 1, 1988.

U.S. Geological Survey: "Management and Use of Small Computer Systems, " Handbook 500-16 - H, July 1985:

–Requires small computers to be physically secured during nonbusiness hours or when left unattended.
–Requires backup copies of vital data stored in a separate location.
–Requires users and owners to conduct a risk analysis.

Department of Defense: "Security Requirements for Automatic Data Processing Systems, Directive 5200.28, December 18, 1972 (with revisions, April 29, 1978):

–Emphasizes that ADP systems must be designed with security in mind, and acknowledges the difficulty of adding security measures to systems already in place.
–Describes in very brief and general terms principles for ADP security needs for systems with

different levels of classified information and users with varying levels of security clearances.
–Directs the Assistant Secretary of Defense (Comptroller) to develop and update a manual for ADP security, and to establish a central DOD capability to assist and advise defense agencies in ADP security.
–Requires the head of each DOD component to designate an official to review ADP applications and approve their security safeguards.
–Sets broad goals for ADP security–individual accountability, environmental control, system stability, data integrity, system reliability, communication link security, and appropriate handling of classified material.

APPENDIX 4B.–HIGHLIGHTS OF FINDINGS ON INFORMATION VULNERABILITY BY THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA)

1. There is no standardized concept of "information sensitivity" among the agencies, and government employees generally are unfamiliar with the term . . . . In contrast to the strong formal programs of [national] security education administered by most agencies, employees are not at all trained in identifying unclassified information which must be protected. [Exceptions include some aspects of protecting documents classified "For Official Use Only" or covered by the Privacy Act.]
2. There is minimal awareness of the vulnerabilities of agency telecommunication facilities to interception.
3. The general failure of government employees and managers to appreciate the threat to vulnerable telecommunications is understandable. Much of the information available on suspected threats to government communications derives from intelligence sources and is classified. It is quite possible, however, to educate employees about potential threats without divulging any classified information.
4. Unclassified information is freely communicated over unprotected circuits without regard to sensitivity.
5. Available telecommunications protection resources are underused or are not used at all.
6. Some stereotyped communications patterns compound the vulnerability problems, [such as] regularly scheduled conference calls which link agencies' top management over private circuits . . . and the use of fixed radio frequencies.
7. A reliance on private lines adds to the vulnerability of sensitive telecommunications ... , The problems facing the would-be interceptor are drastically reduced by the use of leased circuits as opposed to the use of the public network.
8. Communication systems managers are currently unprepared to take on the foregoing problems.
9. Federal law enforcement activities present an entirely different perspective to the general problems of threat and vulnerability . . . . Several law enforcement agencies are seeking equipment solutions to the vulnerability problems they perceive. NTIA notes that these approaches are uncoordinated.

SOURCE: National Telecommunications and Information Administration, "Summary of Findings of Telecommunications and Information Vulnerability Surveys," Mar. 18, 1983.