Appendix B: Federal Information Security and the Computer Security Act

B

This appendix draws on chapter 4 of the September 1994 OTA report *Information Security and Privacy in Network Environments*,[1] with updates as noted herein. That chapter of the 1994 report examined the policy framework within which federal agencies formulate and implement their information-security and privacy policies and guidelines. Because of its importance for federal government information security and cryptography policy, the Computer Security Act of 1987 (Public Law 100-235) was examined in detail.

The Computer Security Act of 1987 established a federal government computer-security program that would protect sensitive information in federal government computer systems and would develop standards and guidelines for unclassified federal computer systems to facilitate such protection. Specifically, the Computer Security Act assigned responsibility for developing government-wide, computer-system security standards and guidelines and security-training programs to the National Bureau of Standards (now the National Institute of Standards and Technology, or NIST). The act also established a Computer System Security and Privacy Advisory Board within the Commerce Department. Additionally, the act required federal agencies to identify computer systems containing sensitive information, to develop security plans for identified systems, and to provide periodic training in computer security for all federal employees and contractors who manage, use, or operate federal computer systems.

In *Information Security and Privacy in Network Environments*, OTA found that implementation of the Computer Security Act has been problematic (see chapter 4 of the 1994 report). In workshop discussions and interviews during and after the assessment, OTA found strong sentiment that agencies follow the rules set forth by the act regarding security plans and training, but do not necessarily fulfill the *intent* of the act. For example, agencies are required to develop security plans—and do—but may not "do the plan" or update plans and implementation in a timely fashion to reflect changes in technology or operations (see section on implementation issues below).

[1] U.S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments*, OTA-TCT-606 (Washington, DC: U.S. Government Printing Office, September 1994).

Implementation of the Computer Security Act has been especially controversial regarding the roles of NIST and National Security Agency (NSA) in standards development for unclassified federal computer systems. The act was designed to balance national security and other national objectives, giving what is now the National Institute of Standards and Technology the lead in developing security standards and guidelines and defining the role of NSA as technical advisor to NIST.[2] However, events subsequent to the act have not convincingly demonstrated NIST's leadership in this area. In OTA's view, NSA has enjoyed de facto leadership in the development of cryptographic standards and technical guidelines for unclassified information security, and implementation of the act has not fulfilled congressional intent in this respect.[3]

EVOLUTION OF POLICY FRAMEWORK FOR UNCLASSIFIED INFORMATION SECURITY[4]

Statutory guidance on safeguarding information provides a policy framework—in terms of technical and institutional requirements and managerial responsibilities—for government information and information-system security. Overlaid on this are statutory privacy requirements that set forth policies concerning the dissemination and use of certain types of information about individuals. Within this framework, and subject to their own specific statutory requirements, federal agencies and departments develop their policies and guidelines, in order to meet individual and government-wide security and privacy objectives.

The **Privacy Act of 1974** (Public Law 93-579) set forth data collection, confidentiality, procedural, and accountability requirements federal agencies must meet to prevent unlawful invasions of personal privacy, and provides remedies for noncompliance. It does not mandate use of specific technological measures to accomplish these requirements. Other statutes set forth information confidentiality and integrity requirements for specific agencies, such as the Internal Revenue Service, Bureau of the Census, and so forth. (Issues related to the Privacy Act, and other, international privacy issues are discussed in chapter 3 of the 1994 OTA report.)

The **Brooks Act of 1965** (Public Law 89-306) was enacted to "provide for the economic and efficient purchase, lease, maintenance, operation, and utilization of automatic data processing [ADP] equipment by federal departments and agencies." *[OTA note: New procurement legislation in the 104th Congress may supersede the Brooks Act.]* The Warner Amendment (Public Law 97-86) subsequently exempted certain types of Defense Department procurements from the Brooks Act (and from section 111 of the Federal Property and Administrative Services Act of 1949).

Among other provisions, the Brooks Act made the Commerce Department the focal point for promulgation of government "automatic data processing" (i.e., computer and information-system) standards and authorized Commerce to conduct a research program to support standards development and assist federal agencies in implementing these standards. These responsibilities were car-

---

[2] NIST recommends standards and guidelines to the Secretary of Commerce for promulgation. Such standards and guidelines would apply to federal computer systems, except for: 1) those systems excluded by section 2315 of Title 10, USC or section 3502(2) of Title 44, USC; and 2) those systems protected at all times by procedures established for information classified by statute or executive order (Public Law 100-235, section 3). The first, "Warner Amendment," exclusion pertains, for example, to intelligence or national security cryptologic systems, mission-critical military or intelligence systems, or systems involving the direct command and control of military forces.

[3] See OTA, op. cit., footnote 1, pp. 138-148, 182-184. See also U.S. General Accounting Office, *Communications Privacy: Federal Policy and Actions,* GAO/OSI-94-2 (Washington, DC: U.S. Government Printing Office, November 1993).

[4] This is taken from OTA, op. cit., footnote 1, ch. 4, esp. pp. 132-138.

ried out by the National Bureau of Standards (now NIST).

NBS established its program in computer and communications security in 1973, under authority of the Brooks Act; the agency was already developing performance standards for government computers. This security program led to the adoption of the Data Encryption Standard (DES) as a federal information processing standard (FIPS) for use in safeguarding unclassified information. The security responsibilities of what is now NIST's Computer Systems Laboratory (CSL) were affirmed and extended by the Computer Security Act of 1987.

The **Paperwork Reduction Act of 1980** (Public Law 96-511) gave agencies a broad mandate to perform their information-management activities in an efficient, effective, and economical manner. [*OTA note: The Paperwork Reduction Act of 1995 was reported on April 3, 1995, and was cleared for the White House on April 6, 1995. The 1995 legislation is discussed in chapter 4 of this background paper. The historical discussion below refers to the 1980 law.*]

The Paperwork Reduction Act of 1980 assigned the Office of Management and Budget (OMB) responsibilities for maintaining a comprehensive set of information resources management policies and for promoting the use of information technology to improve the use and dissemination of information by federal agencies. OMB was given authority for the following: developing and implementing uniform and consistent information resource management policies; overseeing the development of and promoting the use of government information management principles, standards, and guidelines; evaluating the adequacy and efficiency of agency information management practices; and determining whether these practices comply with the policies, principles, standards, and guidelines promulgated by the director of OMB.

OMB Circular A-130 ("Management of Federal Information Resources") was originally issued in 1985 to fulfill these and other statutory requirements (including the Privacy Act). Circular A-130 revised and consolidated policies and procedures from several other OMB directives, which were rescinded. OMB Circular A-130 has recently been revised. The first stage of revisions (June 1993) focused on information exchanges with the public; the second stage addressed agency management practices for information technology and information systems (July 1994). The third stage, addressing security controls and responsibilities in Appendix III of the circular, is ongoing at this writing.

[OTA note: The historical overview of policy development below refers to the 1985 version of Appendix III. OMB's 1995 proposed revision of Appendix III is discussed in chapter 4 of this background paper.]

Appendix III of OMB Circular A-130 (1985) addressed the "Security of Federal Automated Information Systems." Its purpose was to establish a minimal set of controls to be included in federal information systems security programs, assign responsibilities for the security of agency information systems, and clarify the relationship between these agency controls and security programs and the requirements of OMB Circular A-123 ("Internal Control Systems"). The 1985 appendix also incorporated responsibilities from applicable national security directives.

Section 4(a) of the 1985 version of the security appendix of OMB Circular A-130 assigned the Commerce Department responsibility for:

1. developing and issuing standards and guidelines for assuring the security of federal information systems;
2. establishing standards "approved in accordance with applicable national security directives," for systems used to process "sensitive" information, "the loss of which could adversely affect the national security interest;" and
3. providing technical support to agencies in implementing Commerce Department standards and guidelines.

According to the 1985 Appendix III, the Defense Department was to act as the executive agent of the government for the security of telecommunications and information systems that process information, "the loss of which could adversely

affect the national security interest" (i.e., including information that was unclassified but was considered "sensitive"), and was to provide technical material and assistance to federal agencies concerning the security of telecommunications and information systems.

These responsibilities later shifted (see below) in accordance with the Computer Security Act of 1987 and the subsequent National Security Directive 42 (NSD 42). After the Computer Security Act was enacted, NSD 42 set the leadership responsibilities of the Commerce and Defense Departments according to whether the information domain was outside or within the area of "national security."[5]

The **Computer Security Act of 1987** (Public Law 100-235) affirmed and expanded the computer-security research and standards responsibilities of NBS (now NIST) and gave it the responsibility for developing computer system security training programs and for commenting on agency computer system security plans. The Computer Security Act is particularly important because it is fundamental to the development of federal standards for safeguarding unclassified information, to the balance between national security and other objectives in implementing security and privacy policies within the federal government, and to issues concerning government control of cryptography. Moreover, review of the controversies and debate surrounding the Computer Security Act—and subsequent controversies over its implementation—provides background for understanding current issues.

THE COMPUTER SECURITY ACT[6]

The Computer Security Act of 1987 (Public Law 100-235)[7] was a legislative response to overlapping responsibilities for computer security among several federal agencies, heightened awareness of computer security issues, and concern over how best to control information in computerized or networked form. As noted above, the act established a federal government computer-security program that would protect sensitive information in federal government computer systems and would develop standards and guidelines for unclassified federal computer systems to facilitate such protection.[8] Additionally, the act required federal agencies to identify computer systems containing sensitive information, to develop security plans for identified systems, and to provide periodic training in computer security for all federal employees and contractors who manage, use, or operate federal computer systems. The act also established a Computer System Security and Privacy Advisory Board within the Commerce De-

---

[5] The Computer Security Act of 1987 gave the Commerce Department responsibility in information domains that contained information that was "sensitive" but not classified for national security purposes. National Security Directive 42 *(National Policy for the Security of National Security* [emphasis added] *Telecommunications and Information Systems,* July 5, 1990) established a National Security Telecommunications and Information Systems Security Committee (NSTISSC), made the Secretary of Defense the Executive Agent of the Government for National Security Telecommunications and Information Systems, and designated the Director of NSA as the National Manager for National Security Telecommunications and Information Systems. *[OTA note: This information-security structure may be superseded by a new structure under the Security Policy Board, wherein NSTISSC's functions would be incorporated into the functions of a new Information Systems Security Committee. See chapter 4 and box 1-3 of this paper for discussion of the Security Policy Board.]*

[6] This is taken from OTA, op. cit., footnote 1, ch. 4. See pp. 140-142 of that report for legislative history of the Computer Security Act.

[7] 101 Stat. 1724.

[8] The act was "[t]o provide for a computer standards program within the National Bureau of Standards, to provide for government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of federal computer systems, and for other purposes" (ibid.). Specifically, the Computer Security Act assigned responsibility for developing government-wide, computer-system security standards and guidelines and security-training programs to the National Bureau of Standards (now the National Institute of Standards and Technology). NBS (now NIST) would recommend these to the Secretary of Commerce for promulgation.

partment. (The Computer Security Act and a controversial 1989 Memorandum of Understanding (MOU) laying out the working relationship between NIST and NSA to implement the act are contained in appendix B of the 1994 OTA report).

Congressional concerns and public awareness created a climate conducive to passage of the Computer Security Act of 1987. Highly publicized incidents of unauthorized users, or "hackers," gaining access to computer systems and a growing realization of the government's dependence on information technologies renewed national interest in computer security in the early 1980s.[9]

Disputes over how to control unclassified information also prompted passage of the act. The Reagan Administration had sought to give the National Security Agency much control over what was termed "sensitive, but unclassified" information, while the public—especially the academic, banking, and business communities—viewed NSA as an inappropriate agency for such responsibility. The Reagan Administration favored an expanded concept of national security.[10] This expanded concept was embodied in subsequent presidential policy directives (see below), which in turn expanded NSA's control over computer security. Questions regarding the role of NSA in security for unclassified information, the types of information requiring protection, and the general amount of security needed, all divided the Reagan Administration and the scientific community in the 1980s.[11]

Agency Responsibilities Before the Act

Some level of federal computer-security responsibility rests with the Office of Management and Budget, the General Services Administration (GSA), and the Commerce Department (specifically NIST and the National Telecommunications and Information Administration (NTIA)). OMB maintains overall responsibility for computer security policy.[12] GSA issues regulations for physical security of computer facilities and oversees technological and fiscal specifications for security hardware and software.[13] In addition to its other responsibilities, NSA traditionally has been responsible for security of information that is classified for national security purposes, including Defense Department information.[14] Under the Brooks Act, Commerce develops the federal information processing standards that provide specific codes, languages, procedures, and techniques for use by federal information systems managers.[15] NTIA serves as the executive branch developer of federal telecommunications policy.[16]

These overlapping agency responsibilities hindered the development of one uniform federal policy regarding the security of unclassified information, particularly because computer security

---

[9] U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Management, Security and Congressional Oversight,* OTA-CIT-297 (Washington, DC: U.S. Government Printing Office, February 1986), pp. 64-65.

[10] See, e.g., Harold Relyea, *Silencing Science: National Security Controls and Scientific Communication* (Norwood, NJ: Ablex, 1994).

[11] See, e.g., John T. Soma and Elizabeth J. Bedient, "Computer Security and the Protection of Sensitive but Not Classified Data: The Computer Security Act of 1987," *Air Force Law Review,* vol. 30, 1989, p. 135.

[12] U.S. Congress, House of Representatives, Committee on Science, Space, and Technology, *Computer Security Act of 1987—Report to Accompany H.R. 145,* H. Rept. 100-153, Part I, 100th Cong., 1st sess., June 11, 1987 (Washington, DC: U.S. Government Printing Office, 1987), p. 7.

[13] Ibid.

[14] Ibid.

[15] Ibid. The FIPS apply to federal agencies, but some, like the DES, have been adopted in voluntary, industry standards and are used in the private sector. The FIPS are developed by NIST and approved by the Secretary of Commerce.

[16] Ibid.

and communications security historically have developed separately. In 1978, OMB had issued Transmittal Memorandum No. 1 (TM-1) to its Circular A-71, which addressed the management of federal information technology.[17] TM-1 required federal agencies to implement computer security programs, but a 1982 General Accounting Office (GAO) report concluded that Circular A-71 (and its TM-1) had failed to provide clear guidance.[18]

Executive orders in the 1980s, specifically the September 1984 National Security Decision Directive 145, "National Policy on Telecommunications and Automated Information Systems Security" (NSDD-145),[19] created significant shifts and overlaps in agency responsibilities. Resolving these was an important objective of the Computer Security Act. NSDD-145 addressed safeguards for federal systems that process or communicate unclassified, but "sensitive" information. NSDD-145 established a Systems Security Steering Group to oversee the directive and its implementation, and an interagency National Telecommunications and Information Systems Security Committee (NTISSC) to guide implementation under the direction of the steering group.[20]

Expanded NSA Responsibilities Under NSDD-145

In 1980, Executive Order 12333 had designated the Secretary of Defense as Executive Agent of the Government for Communications Security. NSDD-145 expanded this role to encompass telecommunications and information systems security and responsibility for implementing policies developed by NTISSC. The Director of NSA was designated National Manager for Telecommunications and Automated Information Systems Security. The national manager was to implement the Secretary of Defense's responsibilities under NSDD-145. As a result, NSA was charged with examining government information and telecommunications systems to evaluate their vulnerabilities, as well as with reviewing and approving all standards, techniques, systems, and equipment for telecommunications and information systems security.

In 1985, the Office of Management and Budget issued another circular concerning computer security. This OMB Circular A-130, "Management of Federal Information Resources," revised and superseded Circular A-71 (see previous section). OMB Circular A-130 defined security, encouraged agencies to consider information security essential to internal control reviews, and clarified the definition of "sensitive" information to include information "whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission . . . ."[21]

In 1986, presidential National Security Adviser John Poindexter[22] issued "National Telecommunications and Information Systems Security Policy Directive No. 2" (NTISSP No. 2). NTISSP No. 2 proposed a new definition of "sensitive but unclassified information." It potentially could have restricted access to information that previously had been available to the public. Specifically, "sensitive but unclassified information," within the meaning set forth in the directive, included not only information which, if revealed, could adversely affect national security, but also

---

[17] Office of Management and Budget, Transmittal Memorandum No. 1 to OMB Circular A-71, 1978.

[18] U.S. General Accounting Office, *Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices* (Washington, DC: U.S. Government Printing Office, 1982).

[19] NSDD-145 is classified. An unclassified version was used as the basis for this discussion.

[20] This became the National Security Telecommunications and Information Systems Security Committee, or NSTISSC. See footnote 5.

[21] Office of Management and Budget, OMB Circular A-130 (1985). At this writing, the proposed revision of Appendix III of A-130 had just been published. The main section of A-130 was revised and issued in 1993.

[22] Adm. Poindexter was also chairman of the NSDD-145 Systems Security Steering Group (NSDD-145, sec. 4).

information that could adversely affect "other federal government interests" if released. Other federal government interests included economic, financial, technological, industrial, agricultural, and law enforcement interests.

Such an inclusive directive sparked enormous, negative public response. As the Deputy Director of NBS stated during 1987 hearings on the Computer Security Act, the NTISSP No. 2 definition of sensitive information was a "totally inclusionary definition. . . [t]here is no data that anyone would spend money on that is not covered by that definition."[23] Opponents of NSDD-145 and NTISSP No. 2 argued that NSA should not have control over federal computer security systems that did not contain classified information.[24] The business community, in particular, expressed concern about NSA's ability and suitability to meet the private sector's needs and hesitated to adopt NSA's cryptographic technology in lieu of the DES. At the time, the DES was up for recertification.[25] In the House Report accompanying H.R. 145, the Committee on Science, Space and Technology noted that:

> NSDD-145 can be interpreted to give the national security community too great a role in setting computer security standards for civil agencies. Although the [Reagan] Administration has indicated its intention to address this issue, the Committee felt it is important to pursue a legislative remedy to establish a civilian authority to develop standards relating to sensitive, but unclassified data.[26]

In its explanation of the bill, the committee also noted that:

> One reason for the assignment of responsibility to NBS for developing federal computer system security standards and guidelines for sensitive information derives from the committee's concern about the implementation of National Security Decision Directive-145.
>
> . . . While supporting the need for a focal point to deal with the government computer security problem, the Committee is concerned about the perception that the NTISSC favors military and intelligence agencies. It is also concerned about how broadly NTISSC might interpret its authority over "other sensitive national security information." For this reason, H.R. 145 creates a civilian counterpart, within NBS, for setting policy with regard to unclassified information. . . NBS is required to work closely with other agencies and institutions such as NSA, both to avoid duplication and to assure that its standards and guidelines are consistent and compatible with standards and guidelines developed for classified systems; but the final authority for developing the standards and guidelines for sensitive information rests with the NBS.[27]

In its report on H.R. 145, the Committee on Government Operations explicitly noted that the bill was "neutral" with respect to public disclosure of information and was not to be used by agencies to exercise control over privately owned information, public domain information, or information

---

[23] Raymond Kammer, Deputy Director, National Bureau of Standards, testimony, "*Computer Security Act of 1987: Hearings on H.R. 145 Before the Subcommittee on Legislation and National Security of the House Committee on Government Operations*," 100th Cong., 1st Sess., Feb. 26, 1987. See also H. Rept. 100-153, Part I, op. cit., footnote 12, p. 18.

[24] See U.S. Congress, House of Representatives, Committee on Science, Space and Technology, *Computer Security Act of 1987: Hearings on H.R. 145 Before the Subcommittee on Science, Research, and Technology and the Subcommittee on Transportation, Aviation, and Materials of the House Committee on Science, Space, and Technology,* 100th Cong., 1st sess. (Washington, DC: U.S. Government Printing Office, 1987), pp. 146-191.

[25] Despite NSA's desire to replace the DES with a family of tamper proof cryptographic modules using classified algorithms, the DES was reaffirmed in 1988.

[26] H. Rept. 100-153, Part I, op. cit., footnote 12, p. 22.

[27] Ibid., p. 26.

disclosable under the Freedom of Information Act or other laws.[28] Furthermore, the committee noted that H.R. 145 was developed in large part to ensure the delicate balance between "the need to protect national security and the need to pursue the promise that the intellectual genius of America offers us." [29] The committee also noted that:

> Since it is a natural tendency of DOD to restrict access to information through the classification process, it would be almost impossible for the Department to strike an objective balance between the need to safeguard information and the need to maintain the free exchange of information.[30]

Subsequent to the Computer Security Act of 1987, the Defense Department's responsibilities under NSDD-145 were aligned by National Security Directive 42 to cover "national security" telecommunications and information systems.[31] NSD 42 did not rescind programs, such as those begun under NSDD-145, that pertained to national security systems, but these were not construed as applying to systems within the purview of the Computer Security Act of 1987.[32]

NSD 42 established the National Security Telecommunications and Information Systems Security Committee, made the Secretary of Defense the Executive Agent of the Government for National Security Telecommunications and Information Systems, and designated the Director of NSA the National Manager for National Security Telecommunications and Information Systems.[33] As such, the NSA Director was to coordinate with NIST in accordance with the Computer Security Act of 1987.

[*OTA note: The proposal for a new, government-wide centralization of unclassified information security, as presented in the November 1994 Security Policy Board staff report, would place the functions of NSTISSC, along with OMB's functions pursuant to Circular A-130, within a new Information Systems Security Committee chaired by DOD and OMB, with NSA as the secretariat. The staff report noted that this was contrary to the Computer Security Act and suggested the need for a strategy to ensure a "smooth transition" to the new structure, including creating a new definition for "national security related information.[34]" See chapter 4 and box 1-3 of this background paper for discussion of the Board staff proposal, along with discussions of other developments, including OMB's proposed revision of Appendix III of OMB Circular A-130 and the Paperwork Reduction Act of 1995.*]

Agency Information-System Security Responsibilities Under the Act

Under the Computer Security Act of 1987, all federal agencies are required to identify computer systems containing sensitive information, and to develop security plans for identified systems.[35] The act also requires mandatory periodic training in computer security for all federal employees and contractors who manage or use federal computer systems. The Computer Security Act gives final

---

[28] U.S. Congress, House of Representatives, Committee on Government Operations, *Computer Security Act of 1987—Report to Accompany H.R. 145*, H. Rept. 100-153, Part II, 100th Cong., 1st sess., June 11, 1987 (Washington, DC: U.S. Government Printing Office, 1987), p. 30.

[29] Ibid., p. 29.

[30] Ibid., p. 29.

[31] National Security Directive 42, op. cit., footnote 5. The National Security Council released an unclassified, partial text of NSD 42 to the Computer Professionals for Social Responsibility on April 1, 1992, in response to Freedom of Information Act (FOIA) requests made in 1990.

[32] Ibid., section 10. The Warner Amendment (Public Law 97-86) had exempted certain types of Defense Department procurements from the Brooks Act.

[33] NSD 42 (unclassified partial text), op. cit., footnote 31, sections 1-7.

[34] Security Policy Board Staff, "Creating a New Order in U.S. Security Policy," Nov. 21, 1994, pp. 17-18.

[35] Public Law 100-235, section 6.

authority to NIST [then NBS] for developing government-wide standards and guidelines for unclassified, sensitive information, and for developing government-wide training programs.

In carrying out these responsibilities, NIST can draw upon the substantial expertise of NSA and other relevant agencies. Specifically, NIST is authorized to "coordinate closely with other agencies and offices," including NSA, OTA, DOD, the Department of Energy, GAO, and OMB.[36] This coordination is aimed at "assur[ing] maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy" and assuring that NIST's computer security standards are "consistent and compatible with standards and procedures developed for the protection of information in federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."[37] Additionally, the Computer Security Act authorizes NIST to "draw upon computer system technical security guidelines developed by [NSA] to the extent that [NIST] determines that such guidelines are consistent with the requirements for protecting sensitive information in federal computer systems."[38] The act expected that "[t]he method for promulgating federal computer system security standards and guidelines is the same as for non-security standards and guidelines." [39] The intent of the act was that NSA not have the dominant role and to recognize the potential market impact of federal security standards:

> . . . [I]n carrying out its responsibilities to develop standards and guidelines for protecting sensitive information in federal computer systems and to perform research, NBS [now NIST] is required to draw upon technical security guidelines developed by the NSA to the extent that NBS determines that NSA's guidelines are consistent with the requirements of civil agencies. The purpose of this language is to prevent unnecessary duplication and promote the highest degree of cooperation between these two agencies. NBS will treat NSA technical security guidelines as advisory, however, and, in cases where civil agency needs will best be served by standards that are not consistent with NSA guidelines, NBS may develop standards that best satisfy the agencies' needs.
>
> It is important to note the computer security standards and guidelines developed pursuant to H.R. 145 are intended to protect sensitive information in Federal computer systems. Nevertheless, these standards and guidelines will strongly influence security measures implemented in the private sector. For this reason, NBS should consider the effect of its standards on the ability of U.S. computer system manufacturers to remain competitive in the international marketplace.[40]

In its report accompanying H.R. 145, the Committee on Government Operations noted that:

> While the Committee was considering H.R. 145, proposals were made to modify the bill to give NSA effective control over the computer standards program. The proposals would have charged NSA with the task of developing "technical guidelines," and forced NBS to use these guidelines in issuing standards.
>
> Since work on technical security standards represents virtually all of the research effort being done today, NSA would take over virtually the entire computer standards from the National

---

[36] Ibid., section 3(b)(6).

[37] Ibid.

[38] Ibid.

[39] H. Rept. 100-153, Part I, op. cit., footnote 12, p. 26. According to NIST, security FIPS are issued in the same manner as for nonsecurity FIPS. Although the Escrowed Encryption Standard (EES) has classified references, it had the same promulgation method. (F. Lynn McNulty, Associate Director for Computer Security, NIST, personal communication, Mar. 21, 1995.)

[40] Ibid., p. 27.

> Bureau of Standards. By putting NSA in charge of developing technical security guidelines (software, hardware, communications), NBS would be left with the responsibility for only administrative and physical security measures—which have generally been done years ago. NBS, in effect, would on the surface be given the responsibility for the computer standards program with little to say about most of the program—the technical guidelines developed by NSA.
>
> This would jeopardize the entire Federal standards program. The development of standards requires interaction with many segments of our society, i.e., government agencies, computer and communications industry, international organizations, etc. NBS has performed this kind of activity very well over the last 22 years [since enactment of the Brooks Act of 1965]. NSA, on the other hand, is unfamiliar with it. Further, NSA's products may not be useful to civilian agencies and, in that case, NBS would have no alternative but to issue standards based on these products or issue no standards at all.[41]

The Committee on Government Operations also noted the concerns of industry and the research community regarding the effects of export controls and NSA involvement in private sector activities, including restraint of innovation in cryptography resulting from reduced incentives for the private sector to invest in independent research, development, and production of products incorporating cryptography.[42]

The Computer Security Act of 1987 established a Computer System Security and Privacy Advisory Board (CSSPAB) within the Commerce Department:

> The chief purpose of the Board is to assure that NBS receives qualified input from those likely to be affected by its standards and guidelines, both in government and the private sector. Specifically, the duties of the Board are to identify emerging managerial, technical, administrative and physical safeguard issues relative to computer systems security and privacy and to advise the NBS and the Secretary of Commerce on security and privacy issues pertaining to federal computer systems.[43]

The Chair of the CSSPAB is appointed by the Secretary of Commerce. The Board is required to report its findings relating to computer systems security and privacy to the Secretary of Commerce, the OMB Director, the NSA Director, the House Committee on Government Operations, and the Senate Committee on Governmental Affairs.[44]

Implementation Issues

Implementation of the Computer Security Act has been controversial, particularly with respect to the roles of NIST and NSA in standards development. The two agencies developed a Memorandum of Understanding in 1989 to clarify the working relationship, but this MOU has been controversial as well, because of concerns in Congress and elsewhere that its provisions cede NSA much more authority than the act had granted or envisioned.[45] Chapter 4 of the 1994 OTA report examined these implementation issues in depth. It concluded that clear policy guidance and congressional oversight

---

[41] H. Rept. 100-153, Part II, op. cit., footnote 28, pp. 25-26.

[42] Ibid., pp. 22-25, 30-35. In 1986, NSA had announced a program to develop tamper proof cryptographic modules that qualified communications manufacturers could embed in their products. NSA's development of these embeddable modules was part of NSA's Development Center for Embedded COMSEC Products. (NSA press release for Development Center for Embedded COMSEC Products, Jan. 10, 1986.)

[43] H. Rept. 100-153, Part I, op. cit., footnote 12, pp. 27-28.

[44] Public Law 100-235, section 3.

[45] The manner in which NIST and NSA planned to execute their functions under the Computer Security Act of 1987, as evidenced by the MOU, was the subject of hearings in 1989. See U.S. Congress, House of Representatives, Subcommittee on Legislation and National Security, Committee on Government Operations, *Military and Civilian Control of Computer Security Issues,* 101st Cong., 1st sess., May 4, 1989 (Washington, DC: U.S. Government Printing Office, 1989). The NIST-NSA working relationship has subsequently been raised as an issue, with regard to the EES and the DSS. See OTA, op. cit., footnote 1, ch. 4 and app. C.

will be needed if NIST/NSA processes and outcomes are to reflect a different balance of national security and other objectives, or more openness, than have been evidenced since 1989.

The Computer Security Act of 1987 requires all federal agencies to identify computer systems containing sensitive information, and to develop security plans for these systems.[46] The act also requires mandatory periodic training in computer security for all federal employees and contractors who manage, use, or operate federal computer systems. In its workshops and discussions with federal employees and knowledgeable outside observers, OTA found that these provisions of the Computer Security Act are viewed as generally adequate as written, but that their implementation can be problematic.[47]

During the course of the assessment and follow-on work, OTA found strong sentiment that agencies follow the rules set forth by the Computer Security Act, but not necessarily the full intent of the act. In practice, there are both insufficient incentives for compliance and insufficient sanctions for noncompliance with the spirit of the act. For example, though agencies do develop the required security plans, the act does not require agencies to review them periodically or update them as technologies or circumstances change. One result of this is that "[s]ecurity of systems tends to atrophy over time unless there is a stimulus to remind agencies of its importance."[48] Another result is that agencies may not treat security as an integral component when new systems are being designed and developed.

Ongoing NIST activities in support of information security and privacy are conducted by NIST's Computer Systems Laboratory. In the 1994 report, OTA noted that NIST's funding for these security functions ($4.5 million in appropriated funds for FY 1995) has chronically been low, given NIST's responsibilities under the Computer Security Act. "Reimbursable" funds received from other agencies (mainly DOD) have been substantial ($2.0 million in FY 1995) compared with appropriated funds for security-related activities. Since FY 1990, they have represented some 30 to 40 percent of the total funding for computer-security activities and staff at CSL. This is a large fraction of what has been a relatively small budget (about $6.5 million total in FY 1995).

Some of the possible measures to improve implementation were mentioned during OTA staff interviews and workshops circa 1993-94 including the following: increasing resources for OMB to coordinate and oversee agency security plans and training; increasing resources for NIST and/or other agencies to advise and review agency security plans and training; setting aside part of agency budgets for information security (to be used for risk assessment, training, development, etc.); and/or rating agencies according to the adequacy and effectiveness of their information-security policies and plans and withholding funds until performance meets predetermined accepted levels.

---

[46] Public Law 100-235, section 6.

[47] Some of the possible measures to improve implementation that were suggested during these discussions were: increasing resources for OMB to coordinate and oversee agency security plans and training; increasing resources for NIST and/or other agencies to advise and review agency security plans and training; setting aside part of agency budgets for information security (to be used for risk assessment, training, development, and so forth); and/or rating agencies according to the adequacy and effectiveness of their information-security policies and plans and withholding funds until performance meets predetermined accepted levels. (Discussions in OTA workshops and interviews, 1993-94.)

[48] Office of Management and Budget (in conjunction with NIST and NSA), "Observations of Agency Computer Security Practices and Implementation of OMB Bulletin No. 90-08: Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information," February 1993, p. 11.