100TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPT 100-153
Part 2

COMPUTER SECURITY ACT OF 1987

JUNE 11, 1987.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. BROOKS, from the Committee on Government Operations, submitted the following

REPORT

[To accompany H.R. 145 which, on January 6, 1987, was referred jointly to the Committee on Science, Space, and Technology, and the Committee on Government Operations]

[Including cost estimate of the Congressional Budget Office]

The Committee on Government Operations, to whom was referred the bill (H.R. 145) to 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, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Security Act of 1987"

SEC. 2. PURPOSE.

(a) IN GENERAL.—The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.

(b) SPECIFIC PURPOSES.—The purposes of this Act are—

(1) by amending the Act of March 3, 1901, to assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and as-

74-019

sistance (including work products) of the National Security Agency, where appropriate.

(2) to provide for promulgation of such standards and guidelines by amending section 111(d) of the Federal Property and Administrative Services Act of 1949.

(3) to require establishment of security plans by all operators of Federal computer systems that contain sensitive information, and

(4) to require mandatory periodic training for all persons involved in management, use or operation of Federal computer systems that contain sensitive information

SEC. 3. ESTABLISHMENT OF COMPUTER STANDARDS PROGRAM.

The Act of March 3, 1901 (15 U.S.C. 271-278h), is amended-

(1) in section 2(f), by striking out "and" at the end of paragraph (18), by striking out the period at the end of paragraph (19) and inserting in lieu thereof and", and by inserting after such paragraph the following

(20) the study of computer systems (as that term is defined in section 20(d) of this Act) and their use to control machinery and processes.",

(2) by redesignating section 20 as section 22, and by inserting after section 19 the following new sections

SEC. 20. (a) The National Bureau of Standards shall—

(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems,

"(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code,

"(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

"(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code, and

(b) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy,

the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

"(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987, and

"(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

"(b) In fulfilling subsection (a) of this section, the National Bureau of Standards is authorized—

"(1) to assist the private sector, upon request, in using and applying the results of the programs and activities under this section;

"(2) to make recommendations, as appropriate, to the Administrator of General Services on policies and regulations proposed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(3) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(4) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987;

"(5) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost effective security and privacy of sensitive information in Federal computer systems; and

"(6) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)—

"(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

"(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a)(3), and (5) 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

"(c) For the purposes of (1) developing standards and guidelines under subsection (a)(3), and (2) performing research and conducting studies under subsection (b)(5), the National Bureau of Standards shall draw on the technical advice and assistance (including work products) of the National Security Agency, where appropriate

"(d) As used in this section—

"(1) the term 'computer system'—

"(A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

"(B) includes—

"(i) computers;

"(ii) ancillary equipment

"(iii) software, firmware, and similar procedures;

"(iv) services, including support services; and

"(v) related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949;

"(2) the term 'Federal computer system'—

"(A) means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system on behalf of the Federal Government to accomplish a Federal function; and

"(B) includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949;

"(3) the term 'operator of a Federal computer system' means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function;

"(4) the term 'sensitive information' means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

"(5) the term 'Federal agency' has the meaning given such term by section 3(b) of the Federal Property and Administrative Services Act of 1949.

"SEC. 21. (a) There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

"(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of who is representative of small or medium sized companies in such industry;

"(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

"(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency

"(b) The duties of the Board shall be—

"(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

"(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

"(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate Committees of the Congress.

"(c) The term of office of each member of the Board shall be four years, except that—

"(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

"(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

"(d) The Board shall not act in the absence of a quorum, which shall consist of seven members.

"(e) Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

"(f) To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency

"(g) As used in this section, the terms 'computer system' and 'Federal computer system' have the meanings given in section 20(d) of this Act. '; and

(3) by adding at the end thereof the following new section:

"SEC. 23. This Act may be cited as the National Bureau of Standards Act."

SEC. 4. AMENDMENT TO BROOKS ACT

Section 111(d) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(d)) is amended to read as follows:

"(d)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 20(a) (2) and (3) of the National Bureau of Standards Act, promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems. The President may disapprove or modify such standards and guidelines if he determines such action to be in the public interest. The President's authority to disapporve or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be submitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

"(2) The head of a Federal agency may employ standards for the cost effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

"(3) The standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or cause a major adverse financial impact on the operator which is not offset by government-wide savings. The Secretary may delegate to the head of one or more Federal agencies authority to waive such standards to the extent to which the Secretary determines such action to be necessary and desirable to allow for timely and effective implementation of Federal computer systems standards. The head of such agency may redelegate such authority only to a senior official designat-

ed pursuant to section 3506(b) of title 44, United States Code. Notice of each such waiver and delegation shall be transmitted promptly to the Committee on Governmental Operations of the House of Representatives and the Committee of Government Affairs of the Senate and shall be published promptly in the Federal Register.

"(4) The Administrator shall revise the Federal information resources management regulations (41 CFR ch. 201) to be consistent with the standards and guidelines promulgated by the Secretary of Commerce under this subsection.

"(5) As used in this subsection, the terms 'Federal computer system' and 'operator of a Federal computer system' have the meanings given in section 20(d) of the National Bureau of Standards Act."

SEC. 5. TRAINING BY OPERATORS OF FEDERAL COMPUTER SYSTEMS.

(a) IN GENERAL.—Each operator of a Federal computer system that contains sensitive information shall provide mandatory periodic training in computer security awareness and accepted computer security practice. Such training shall be provided under the guidelines developed pursuant to section 20(a)(5) of the National Bureau of Standards Act (as added by section 3 of this Act), and in accordance with the regulations issued under subsection (c) of this section, for all employees who are involved with the management, use, or operation of computer systems.

(b) TRAINING OBJECTIVES.—Training under this section shall be started within 60 days after the issuance of the regulations described in subsection (c). Such training shall be designed—

(1) to enhance employees' awareness of the threats to and vulnerability of computer system; and

(2) to encourage the use of improved computer security practices.

(c) REGULATIONS.—Within six months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided under subsection (a) and the manner in which such training is to be carried out.

SEC. 6. ADDITIONAL RESPONSIBILITIES FOR COMPUTER SYSTEMS SECURITY AND PRIVACY.

(a) IDENTIFICATION OF SYSTEMS THAT CONTAIN SENSITIVE INFORMATION.—Within 6 months after the date of enactment of this Act, each Federal agency shall identify each Federal computer system, and system under development, which is within or under the supervision of that agency and which contains sensitive information.

(b) SECURITY PLAN.—Within one year after the date of enactment of this Act, each such agency shall, consistent with the standards, guidelines, policies, and regulations prescribed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949, establish a plan for the security and privacy of each Federal computer system identified by that agency pursuant to subsection (a) that is commensurate with the magnitude of the harm resulting from the loss, misuse, or unathorized acces to or modification of the information contained in such system. Copies of each such plan shall be transmitted to the National Bureau of Standards and the National Security Agency for advice and comment. A summary of such plan shall be included in the agency's five-year plan required by section 3505 of title 44, United States Code. Such plan shall be subject to disapproval by the Director of the Office of Management and Budget. Such plan shall be revised annually as necessary.

SEC. 7. DEFINITIONS.

As used in this Act, the terms "computer system", "Federal computer system", "operator of a Federal computer system", "sensitive information", and "Federal agency" have the meanings given in section 20(d) of the National Bureau of Standards Act (as added by section 3 of this Act).

SEC. 8. RULES OF CONSTRUCTION OF ACT.

Nothing in this Act, or in any amendment made by this Act, shall be construed—

(1) to constitute authority to withhold information sought pursuant to section 552 of title 5, United States Code; or

(2) to authorize any Federal agency to limit, restrict, regulate, or control the collection, maintenance, disclosure, use, transfer, or sale of any information (regardless of the medium in which the information may be maintained) that is—

(A) privately-owned information;

(B) disclosable under section 552 of title 5, United States Code, or other law requiring or authorizing the public disclosure of information; or

(C) public domain information.

The Committee on Government Operations, to whom was jointly referred, along with the Committee on Science, Space, and Technol-

ogy, the bill (H.R. 145) to amend the Act establishing the National Bureau of Standards to assign responsibility for developing standards and guidelines for Federal computer systems, to provide for a computer security research program within such Bureau, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment strikes out all after the enacting clause of the bill and inserts a new text which appears in bold face roman type in the reported bill.

SUMMARY AND PURPOSE

H.R. 145 places a new focus on the need for developing increased awareness of the importance of computer security and the potential loss or disruption of vital government programs that would result from unauthorized access to Federal computers. It would establish a computer standards program within the National Bureau of Standards (NBS) which will be responsible for a government-wide computer security program, and for the training of Federal employees who are involved in the management, operation, and use of computers. The bill establishes a new research program at NBS which will assess the vulnerability of government computers and develop technical and management techniques to defend against unauthorized attempts to gain access to sensitive governmental information.

H.R. 145 is the result of growing concern within the Congress that the government's computer and communications systems are not being adequately protected from unauthorized manipulation and potential destruction. This Committee has over the years conducted extensive investigations of computer and communications facilities of several major Federal agencies. In almost every case, security was lax or virtually non-existent. Notwithstanding, computer and communications security has remained a low priority for most Federal agencies and a relatively small amount of funds has been devoted to this area.

In order to stop what the Administration perceived as a foreign exploitation of our nation's computer-based information systems, the President issued in September of 1984, National Security Decision Directive (NSDD) 145: National Policy on Telecommunications and Automated Information Systems Security. Under this directive, the Department of Defense (DOD) was given broad new powers to issue policies and standards for the safeguarding of not only classified information, but also other information in the civilian agencies and private sector which DOD believed should be protected. The National Security Agency (NSA), whose primary mission is one of monitoring foreign communications, was given the responsibility of managing this program on a day-to-day basis.

The issuance of NSDD-145 raised considerable concern within the private sector and the Congress. First, it expanded DOD's authorities beyond its typical role of protecting classified information to deciding what unclassified information should be protected. Second, it gave NSA the authority to use its considerable foreign intelligence expertise within this country. This is particularly trou-

bling since NSA was not created by the Congress, but by a secret presidential directive and it has, on occasion, improperly targeted American citizens for surveillance. Third, the Directive is in conflict with current law, which assigns authorities and responsibilities for the development of computer and communications standards to agencies other than DOD. Under both the Brooks Act (P.L. 89-306) and the Paperwork Reduction Act (P.L. 96-511), the Office of Management and Budget (OMB), the General Services Administration (GSA), and the Commerce Department have government-wide management and policy responsibilities for computers, telecommunications and information management, including authority for the issuance of policies and standards for computer security.

Last Congress, during its consideration of a similar bill (H.R. 2889, the Computer Security Act of 1986), the Committee noted in its report that "NSA's involvement [in computer standards under NSDD-145] could have a chilling effect on the vigorous research and development that is on-going in the academic community and our domestic computer industry. This industry has been one of the most viable segments of our economy. Its rapid technological advances have been due in large part to being free to openly exchange ideas without government interference. NSA's inherent tendency to classify everything at its highest level is bound to conflict with this broader goal." The Committee further noted that NSA's "activities under the Directive could lead to the obstruction of the free flow of information to our businesses, schools, and citizens—all in the name of national security."

The Committee's concern over the "Big Brother" activities of DOD and NSA was borne out when Admiral Poindexter, then National Security Advisor to the President, issued on October 29, 1986, a policy directive which, in DOD's view, gave legitimacy to the military's efforts to restrict access to unclassified information located in civilian agencies and the private sector. These censorship efforts included visits by CIA, FBI, and NSA agents to private data base companies and libraries to find out who the users of these data bases were, their addresses and to request that these users be surreptitiously monitored when they access these computerized data bases.

H.R. 145 contains provisions to greatly restrict these types of activities by the military intelligence agencies under NSDD-145 and the Poindexter Directive while at the same time providing a statutory mandate for a strong security program headed up by NBS, a civilian agency. During the Committee's consideration of this legislation, NSA opposed its passage and asserted that NSA should be in control of this nation's computer standards program. The Deputy Secretary of Defense and the Secretary of Commerce testified, however, that a civilian agency, NBS, would be in charge of this program. The Director of OMB forwarded a formal administration position to the Committee reiterating the testimony of both the Defense and Commerce Secretaries, that NBS would be in charge. In addition, as a result of the hearings, National Security Advisor Frank Carlucci, Admiral Poindexter's successor, and White House Chief of Staff Howard Baker notified the Committee that the Poindexter Directive was being rescinded and a review of NSDD-145 was being initiated.

The bill assigns to NBS the responsibilities for the establishent of computer and communications security standards on a government-wide basis in accordance with the Brooks Act and the Paperwork Act. NSA is given the statutory role of assisting NBS in its government-wide standard-setting duties. NSA is also allowed to continue its computer security work in those Defense systems which are currently exempted from the Brooks Act and the Paperwork Act. Given the urgent need to protect our nation's computer systems, the Committee fully expects NSA to focus its attention on the task at hand—the development of a strong computer security program.

H.R. 145 requires each agency to identify its own sensitive information which may need protection and, in addition, develop a computer security plan outlining its proposed efforts to protect this information. Copies of the plan are to be sent to both NBS and NSA for advice and comment. The Director of OMB has the authority to disapprove an agency's plan if it is found to be deficient.

H.R. 145 also establishes an advisory board consisting of outside experts, government officials and those in private industry to advise NBS in its work. NSA is required to serve as one of these advisors. Since the development of standards requires a process where varied viewpoints are essential, the Committee would expect the Secretary of Commerce to make sure the Advisory Board is composed of members from a diverse segment of our society, including both the producers and users of this technology.

H.R. 145 requires each Federal agency to provide mandatory, periodic training to Federal employees to increase security awareness and to provide adequate protection for their computer and communications systems.

H.R. 145 contains a presidential review provision whereby the President can direct the Secretary of Commerce to modify or rescind a standard or guidelines if it is in the public interest to do so.

H.R. 145 also contains provisions that make it absolutely clear that nothing in this Act affects the disclosure of information that is currently available to the public via the Freedom of Information Act or any other law.

Committee Action and Vote

H.R. 145 was introduced by Congressman Dan Glickman on January 6, 1987, and subsequently referred jointly to the Committees on Government Operations ordered the bill reported as amended on April 7, 1987, by a voice vote with a quorum present.

Hearings

Hearings on H.R. 145 were held by the Subcommittee on Legislation and National Security on February 25, 26, and March 17, 1987. Testimony was received from Congressmen Dan Glickman (D-Kans.), Glenn English (D-Okla.), Anthony C. Bielenson (D-Calif.), and former Congressman Don Fuqua (D-Fla.). Testimony was also received from representatives of the U.S. General Accounting Office, the American Bankers Association, the American Physical Society, the Institute of Electrical and Electronics Engineers, the American Library Association, the Association of Research Librar-

ies, the Department of Commerce, the Office of Technology Assessment, the Department of Defense, the National Security Agency, the Information Industry Association, the Computer and Communications Industry Association, and the Congressional Research Service of the Library of Congress. Further testimony was provided by Robert H. Courtney, Jr., a private sector consultant on computer security; Dr. David K. Kahn, a recognized expert on the National Security Agency and author of *The Codebreakers*; Malcolm Baldridge, The Secretary of Commerce; and William Howard Taft IV, Deputy Secretary of Defense. Both Rear Admiral John M. Poindexter, former National Security Advisor, and Kenneth de Graffenreid, former Special Assistant to the President for National Security Affairs refused to appear before the Subcommittee, whereby a subpoena was issued to require their attendance at the hearings. In his appearance before the Subcommittee on March 17, 1987, Admiral Poindexter refused to testify on the grounds that it may violate his constitutional rights under the Fifth Amendment. Mr. de Graffenreid did not invoke his constitutional rights and testified as requested.

Explanation of Amendment

Inasmuch as all after the enacting clause of H.R. 145 was stricken and all language incorporated into one amendment, this report constitutes an explanation of the amendment.

Discussion

BACKGROUND

Over the last thirty years, the government has greatly expanded its use of computer and communications technology. Current estimates from the Office of Technology Assessment (OTA) indicate that over $60 billion is spent annually by Federal agencies to acquire, develop and use this technology in automating its operations.[1] Although the information technology revolution has greatly increased the efficiency of government programs at reduced costs, it has also made virtually every agency dependent on its use. Moreover, the potential for abuse of this technology is enormous. For example, information is maintained by the Internal Revenue Service and the Social Security Administration on virtually every citizen of the United States which, if altered, manipulated, or destroyed, could affect the privacy of these individuals. Further, the Federal Reserve System transmits billions of dollars everyday over its communications lines which, if tampered with, could affect the viability of our nation's economy.

During the 1960's and early 1970's, Federal agencies could with a reasonable degree of assurance protect their computer systems and data files because most of the processing was being done at central sites. However, with the advent of mini and micro technology, coupled with on-line access, the aforementioned protection ceased to exist. Today, any knowledgeable computer person can tap into

[1] Federal Government Information Technology: Management, Security, and Congressional Oversight, Office of Technology Assessment, February 1986. Note: OTA estimates the Federal Government has about 27,000 mainframe computer terminals.

almost any computer system thousands of miles away. There have been many stories in the press about hackers who have managed with relative ease to enter a computer system containing sensitive information and manipulate it for their own purposes. School systems, banks and even the Defense Department have not been able to stop these unwarranted intrusions. On a more malicious level, credit card information and even tax records have been altered or destroyed and the use of computers to theft and fraud has been on the rise over the last five years.

Unfortunately, efforts by the Federal Government to establish a computer security program have not kept pace with the rapidly changing technology. Most agencies have placed such a low priority in protecting its computer systems that even the most basic computer security measures, i.e. physical and administrative, do not exist. Not surprisingly, little effort has been made to use the technology itself to secure the computer systems from outside penetration. This lack of computer security is a serious problem since such systems are the core of every modern organization. Destruction of these systems would undoubtedly bring the operations of these organizations to an abrupt halt and the effect of this on our citizens would be catastrophic.

H.R. 145 is designed to establish a credible computer security program for the Federal Government by placing a civilian agency, the National Bureau of Standards (NBS), in charge of development appropriate standards and guidelines to protect the government's vital information systems. It establishes a new research program within the National Bureau of Standards to assess the vulnerability of government computers and communications. It provides for the development of technical and management techniques to defend against unlawful access to sensitive government information and for mandatory training for Federal employees. It also creates a computer security board composed of experts from the government and the private sector and requires agencies to identify sensitive information and develop plans to protect that information. Further, it clearly delineates the roles of NBS and NSA in regard to their responsibilities under the newly-established computer security program. The bill also establishes a presidential review process whereby the Secretary of Commerce can be directed to modify or rescind a standard when the President determines it is in the public interest to do so. Finally, the bill contains provisions which make it perfectly clear that nothing in this Act affects the disclosure of information required under the Freedom of Information Act or any other law.

FEDERAL COMPUTER STANDARDS PROGRAM

With the passage of the Brooks Act (P.L. 89-306) in 1965, the Department of Commerce was given the responsibility for the development and issuance of Federal computer standards. Pursuant to its enactment, the Institute of Computer Sciences and Technology (ICST) was established within the National Bureau of Standards to fulfill the responsibilities given to the Department of Commerce by the Brooks Act. The Paperwork Reduction Act of 1980 (P.L. 96-511) reinforced the role of ICST and the Commerce Department in the

development of computer standards. In recognition of the importance of information technology and the vital role that Federal standards has in using the technology, this law further called on the OMB to revitalize the standards program.

In fulfilling its statutory mandate, the Institute conducts research into and provides technical support to the development of national and international standards for computer software and hardware, including computer networks. Although ICST was originally established to assist the Federal agencies, the Institute has always worked directly with private sector users, vendors, and through the voluntary standards process to disseminate solutions that are applicable to a wide range of users. As a result, the Institute's work has benefited Federal, State and local governments as well as the private sector, particularly our nation's computer industry. It has issued over 125 Federal Information Processing Standards, other important technical guidance documents, and, in addition, provided valuable technical assistance and leadership in both the national and international standards areas.

The Institute recognized as far back as 1972 that computer security would be a major concern for users of the technology. At that time, it initiated its Computer Security and Risk Management program. This program encompasses research into and development of security standards, transfer of technology to potential implementors and vendors, and assistance to users of security technology. Numerous standards, guidelines and technical reports have been issued in the areas of physical security, technical security and computer security management. The institute has also established comprehensive programs in computer reliability and integrity to prevent unauthorized modification of information and to ensure the accuracy of the data stored in computer systems.

Deputy Secretary of Commerce noted the accomplishments made by the Institute during his testimony. He stated that:

> The NBS Institute for Computer Sciences and Technology Computer Security Division develops, validates, and maintains security standards for the Federal Government. For example, NBS played a major role in developing the internationally accepted open system interconnection (OSI) network system architecture which provides the framework for the development of standards for interconnecting a set of computer systems that are manufactured by different vendors. Recently, NBS has begun defining the security components of the OSI architecture. Within that scope, the division is defining, implementing, demonstrating, and testing security standards. These standards provide worldwide security services for protecting data against unauthorized modification, undetected data loss, and unauthorized disclosure, as well as verification of the identities of both the sender and receiver of computer data.
>
> In parallel with the OSI security effort, the NBS computer security division has continued to develop and validate security standards for financial data networks. The division provides technical consultation and produces guidelines and standards to assist other Federal agencies

> and members of the private sector in the evaluation of their security needs and provides recommendations for system implementation and modifications.[2]

Unfortunately, despite the considerable achievements by the Institute, efforts have been made by the Administration over the last six years to cut drastically the funding of this important program. Those cuts are being made without regard to the significant benefits that have been achieved by the program. The issuance of 54 Federal Information Processing Standards (FIPS) by the Institute is saving the government about $132 million annually—thirteen times the annual budget of the Institute.[3] This Committee and the Science, Space, and Technology Committee have worked to ensure continued funding to the Institute over the last six years.

Robert H. Courtney, a private sector computer security consultant, noted during the hearings that despite the funding problems:

> NBS [has] established a highly cooperative endeavor with informal, unfunded representative from several civil agencies, from DOD, from the vendors of data processing gear and programs and from the private sector user community. Some of the most significant measures in place today are a direct consequences of the vendors becoming aware of the needs of the public and private sector user community for those measures. With education, but without regulations, those measures were simply incorporated into the design of the base products. The development by IBM of the cryptographic algorithm which later became the federal data encryption standard, DES, came as a result of IBM's awareness of the need for such a algorithm through its participation in the NBS computer security program.
>
> The standards and guidelines published by NBS over the past dozen years have made a significant contribution to the state of the art in computer security in the federal government.[4]

Clearly, NBS has earned its well-deserved reputation for its work in developing computer standards, including computer security standards. Although often operating on a limited budget, it has managed through its own initiative to fulfill the responsibilities given to it under the Brooks Act and the Paperwork Reduction Act. Given its notable achievements, the Committee would expect OMB to more adequately fund this important program.

NSDD-145

To counter the growing threat of foreign exploitation of computer-based information systems within both the government and the private sector, in September of 1984 the President issued National

---

[2] Statement of Clarence J. Brown, Deputy Secretary of Commerce, dated Feburary 26, 1987, p. 5-6.

[3] These figures were involved by Joe Wright, then Deputy Secretary of Commerce, on October 21, 1981, in testimony before the Subcommittee on Legislation and National Security, Committee on Government Operations.

[4] Statement of Robert H. Courtney, dated February 25-26, 1987, p. 4

Security Decision Directive (NSDD 145). This Directive seeks to vest in the Department of Defense (DOD) the authority to establish policies and standards that would govern the access to and the processing of all computerized information which DOD deems to be critical to the national security of the United States. This would include not only classified information, but any other computerized information within the civilian agencies that the Department considers to be in need of protection in the interest of national security. Under the Directive, virtually any information system located in the civilian agencies or the private sector would fall under its domain.

During the February 1987 hearings, Assistant Secretary of Defense Donald Latham denied that NSDD-145 was a charter for the Defense Department to control access to sensitive unclassified information located in civilian agencies and the private sector.[5] General Odom echoed Mr. Latham's testimony saying that NSDD-145 did not set up NSA as computer security czar and that its only role with the private sector is one of "*encouraging, advising,* and *assisting*" it with its information security needs. The Committee notes that these same assertions were made by Mr. Latham and NSA last Congress during the Committee's review of H.R. 145's predecessor legislation. (Emphasis added.)[6]

In hearings held by the Committee in September 1985, Mr. Latham claimed that NSDD-145 was being misread and that the directive was being misconstrued. He characterized NSDD-145 as a cooperative effort between Federal agencies and the private sector to improve the security of the nation's computers. To accomplish this, NSA and DOD provide advice and assistance. According to Mr. Latham, NSDD-145 is "a much more benign document than others appear to think it is. . . ."[7] In fact, Mr. Latham went to great lengths during the September 1985 hearings to allay the concerns of this Committee and many others that NSDD-145 is intended to give NSA and DOD a free hand to control information throughout the government and the private sector. Mr. Latham also noted "that NSDD-145 does *not cover unclassified but sensitive non-national security-related information* and, therefore, it in no way restricts, controls, or manages the activities of other Federal departments or agencies who have responsibilities in non-national security-related areas."[8] (Emphasis added.)

Notwithstanding, in April 1986, NSA, which reports to Mr. Latham regarding computer security matters, announced that it was merging its Communications Security (COMSEC) and its Computer Security (COMPUSEC) organizations into an integrated organization called Information Security. In its announcement, the following was stated:

> The responsibilities of the new organization [within NSA] are being broadened under the auspices of National

---

[5] Statement of Donald C. Latham, Assistant Secretary of Defense for Command, Control, Communications and Intelligence, February 26, 1987.
[6] H.R. 2889, The Computer Security Act of 1986.
[7] Hearing Record, dated September 18, 1985, p. 62.
[8] Hearing Record, dated September 18, 1985, p. 54. (This and similar statements are *repeated three times* in his written testimony.

> Security Decision Directive 145 *to include all computer security and communication security for the Federal Government and private industry,* including the protection of classified information; unclassified national security sensitive information; and *non-national security sensitive information.*" (Emphasis added.)

This broadening of responsibilities to include all information in the government and the private sector, including non-national security sensitive information was approved on December 20, 1985, by the NSDD-145 Steering Group headed by former National Security Advisor, Admiral Poindexter—barely three months after Mr. Latham testified before the Committee.[9] No effort was made by DOD to notify the Committee of the change in position where important new powers were granted to DOD and NSA as a result of this December 20, 1985, decision.

Poindexter Directive—A move toward censorship

Less than a year later, on October 29, 1986, the then National Security Advisor, Admiral Poindexter, issued (under his own signature) a directive which further expanded DOD's control to a wide spectrum of scientific, economic and cultural information in our nation.[10] This document made no pretense of being an advisory document to the President, and there is no indication that the President even knew about it. This directive was an operational order demanding all agencies of the Federal Government take certain actions. This included defining all unclassified information as "sensitive" if it met the following criteria:

> Sensitive, but unclassified information is information the disclosure, loss, misuse, alternation, or destruction of which could adversely affect national security or other Federal Government interests. National security interests are those unclassified matters that relate to the national defense of the foreign relations of the U.S. Government. *Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens.* (Emphasis added.)
>
> This policy applies to all Federal Executive Branch Departments and Agencies and entities, including their contractors, which electronically transfer, store, process, or communicate sensitive, but unclassified information."[11]

Notwithstanding Latham's repeated assurances over the last three years that NSDD 145 is a bland document and the intent of

[9] Mr. Latham's position under NSDD-145 is illustrated in the chart on page 27.
[10] Admiral Poindexter's position under NSDD-145 is illustrated in the chart on page 27
[11] Poindexter Directive on sensitive information, dated October 29, 1986. This Directive has the formal title of "National Policy on Protection of Sensitive, But Unclassified Information In Federal Government Telecommunications and Automated Information Systems, and is also sometimes referred to as the National Telecommunications and Information Systems Security Policy (NTISSP) No 2.

it is misunderstood, the private sector soon found out what it meant to receive "encouragement, advice and assistance" from the military intelligence agencies. The real intent of NSDD-145 and the Poindexter Directive become readily apparent—even to those who still clung a to DOD's reassurances.

On November 11, 1986, Mr. Latham's deputy for DOD's information systems, in a talk before an information Industry Association convention in New York, said:

> I don't believe that the issue is whether or not we're going to protect information. I believe that the issue is what information we're going to protect both within the Federal Government, both within DOD and also within industry."[12]

On December 10, 1986, the Associate Director of the State University of New York (SUNY-Buffalo) was requied by an FBI initiated subpoena to provide information on the library data base searches conducted by a foreign student. This has had a chilling effect on the library and university communities. If the military intelligence agencies or the FBI can demand to know what data bases students are interested in, then a dossier can be established on each individual doing research in his area of interest. This could lead to increased surveillance over our citizens merely because of the magazines, books or newpapers they read. One question noted by the SUNY-Buffalo library was: How did the FBI know in the first place that the foreign student had conducted such a search of the library's data bases?

During the fall of 1986 under the auspices of NSDD-145, private sector data base companies received visits from CIA, FBI, and NSA agents. Among those companies visited were Mead Data Central, Inc., and Lockheed Corporation's Dialogue. According to testimony from the Information Industry Association,[13] these agents wanted to obtain a list of the users of the on-line data bases that were visited, the addresses of those users, and to install monitors on the communication systems to track which data bases were being accessed and by whom.[14] The American Civil Liberties Union (ACLU) observed during the hearings that the government (for the moment) seemed to be seeking voluntary compliance from the information industry, but appeared willing to use various forms of coercion to achieve its aims. These include:

> Limiting the availability of data on line in government data bases;

---

[12] Even before the Poindexter Directive was signed, Mr Latham was quoted on May 27, 1986, in a Washington Post interview as saying: "I'm very concerned about what people are doing—and not just the Soviet. If that means *putting a monitor on Nexis-type systems*, then I'm all for it . . . The question is how do you do it technically without unnecessary interference." (Emphasis added.)

The term "NEXIS-type systems" refers explicitly to NEXIS, which was developed by Mead Data Central of Ohio. It is a computer-assisted news, business, marketing, and general information retrieval service. Among other information, it contains newspaper stories such as those published in the New York Times.

[13] Hearing transcript, p. 93. Jack Simpson, President of Mead Data Central, testified for the IIA.

[14] Under Executive Order 12333, NSA and CIA are prohibited from conducting foreign counterintelligence or domestic security surveillance of United States citizens or organizations within this country.

Placing selective limits on who may access government data bases;

Monitoring who subscribes or seeks to use government data bases and the nature of their inquiries;

Refusal to release or sell data in electronic form;

Licensing government data base information subject to restrictions on access or further dissemination;

Contracting with private data base companies to provide data base services subject to restrictions on access or further dissemination;

Reclassifying data already disseminated to private data vendors;

Threatening commercial data base firms with prosecution under the export control laws for failure to limit data dissemination." [15]

The implication of such clandestine activity by the military intelligence agencies was immediately felt within the information and library communities—the military was willing to use its power to control sensitive information in the Federal Government and the private sector.[16]

REACTION TO DOD'S EFFORTS TO CONTROL INFORMATION

These activities by DOD and NSA resulted in strong criticism before the Committee from a wide range of witnesses who were deeply concerned that DOD's efforts under NSDD-145 and the Poindexter Directive would restrain, constrict and otherwise strangle the free flow of information in this country—all in the name of national security.

In a letter to the Committee expressing its support for H.R. 145, the Aetna Life and Casualty Company stated its opposition to NSDD-145 as follows:

This directive [NSDD-145] does two things. It gives the Department of Defense (DoD) power to decide what information in civilian agency and private sector computers is sensitive and consequently requires protection. And it gives the National Security Agency operational management of that decisional process. NSDD-145 seems to conflict with P.L. 89-306 (Brooks Act) and P.L. 96-511 (Paperwork Reduction Act) which identify the Office of Management and Budget, the General Services Administration, and the Commerce Department as having management and policy responsibilities for Federal computers, telecommunications, and information management.

Aetna, as any large financial services company, is subject to a sizable body of regulation and law. These statutory requirements are formally and openly stated. To add

[15] Statement of the American Civil Liberties Union, dated February 25, 1987, p. 13

[16] Jack Simpson, President of Mead Data Central, was quoted in published reports as saying "This concern of mine is one that you must share. Until you have received cordial visits by representatives of the FBI, the CIA, and the DOD, you can't appreciate the true extent of this issue."

NSDD-145, a classified instrument we can read only in sanitized, unclassified form, is wrongful regulation. Compliance could affect the pricing of our products and consequently our competitiveness in the market place. We do not believe NSDD-145, as we understand it, is in the public interst. We would strongly urge the President to rescind it.

We feel the National Bureau of Standards is appropriate to perform this function; expert, reputable, effecting sound direction for both government and private sector. We see this security role as extension to work the Bureau performed in establishing the Data Encryption Standard (DES)—a strong, effective algorithm, privately developed, commonly used in government and commercial applications, and fully approved in both sectors. The Bureau's Institute for Computer Science and Technology has, for some time, provided technical guidance in data processing, including security, for the civil agencies of government. This bill will make information systems security a formal NBS objective applying to all Federal government. We fully endorse that objective.[17]

The American Civil Liberties Union witness testified in very strong terms that NSDD-145 and the Poindexter Directive establish a bridgehead for the government to undermine the First Amendment rights given to our citizens in their Constitution. The scientist and engineers were equally vocal in their criticism. They believe the restrictions on the open exchange of scientific ideas are harming, rather than protecting, our national security. They also questioned why the military is trying to establish this policy when we lead the Soviets in 14 out of 20 key technologies and, at worst, are tied in the other six. The witness from the American Banking Association testified that DoD's interference with our nation's banking system has been expensive, highly disruptive and counterproductive. Finally, the representatives of the nation's libraries called NSDD-145 and the Poindexter Directive a dangerous new form of government censorship which cannot be tolerated.[18]

The American Physical Society further noted in its testimony:

At times the U.S. seems intent on emulating the Soviet Union's failed system. Since 1980, the scientific and technical community in the U.S. has fought one skirmish after another with Federal agencies over policies that would constrain the free conduct or reporting of unclassified research: Barring of foreigners from attendance at unclassified conferences; pressuring authors to withdraw unclassified papers from open meetings; inducing researchers in certain fields to submit their unclassified research papers to government agencies for prepublication review; barring

[17] Letter to Chairman Brooks from Irwin J. Sitkin, Vice President, Corporate Administration, Aetna Life Insurance Company, dated February 19, 1987.

[18] Note: The American Library Association (ALA) passed a resolution on January 21, 1987, stating, among other things, that "Libraries should challenge censorship in the fulfillment of their responsibility to provide information and enlightment. . . ." The Association called for the Poindexter Directive to be rescinded.

of foreigners from access to unclassified research facilities.[19]

The witness also observed that:

> One has only to look at our political adversaries to witness the effect of government restraints on scientific debate. Soviet biology trails far behind that of the West, largely as a result of years of official support for the discredited genetic theories of Lysenko. Solid state electronics in the Soviet Union has never fully recovered from the official decisions to stress germanium-based technology over silicon based. It is hard to believe that these decisions could have long persisted in an atmosphere of free discussion. The Department of Defense reports that of twenty key technologies, we lead the Soviets in fourteen, and are at worst tied in the other six. It can be argued that barriers to internal scientific communication have contributed to this imbalance, and have compelled the Soviets to conduct a massive intelligence effort aimed at the acquisition of Western technology.[20]

Congressman Glenn English expressed his concern over the military's unprecedented intrustion into the constitutional rights of our citizens when he testified:

> I do not believe that the national security bureaucracy has done such an exemplary job of protecting classified government information that it should be assigned any responsibility over unclassified, privately owned information. Further, I do not know where the government derives authority to regulate or control privately owned, unclassified information. Doesn't the First Amendment to the Constitution prevent such activity by the government? Finally, I do not understand why the private sector cannot be allowed to provide for the scurity of its own information. If the private companies need help from the government, let them ask for it.
>
> In concluding my statement, I want to refer to the espionage problems that have been so much in the news in the last few years. The espionage cases taught us that we need to classify less information and that we need instead to control classified information more effectively.
>
> This lesson has apparently been lost on the national security establishment. It is not enough for the military bureaucracy to classify millions of documents each year. Now they want to impose restrictions on unclassified information and on privately owned data as well.
>
> The apparently insatiable desire of the military for controlling information—whether classified or unclassified, whether government or private—is the most convincing argument for H.R. 145. One only has to examine the record to understand the need for a legislative rejection of

[19] Statement of the American Physical Society, February 25, 1987, p. 2.
[20] Statement of the American Physical Society, February 25, 1987, p. 2.

the National Security Decision Directive and for preserving civilian agency management of civilian information."[21]

All of the aforementioned witnesses strongly supported the need for H.R. 145. They believe that Congress must reestablish civilian control over the government's computer security program. They urged Congress to restore the critical balance between the need to protect vital data from misuse while at the same time ensuring the free flow of information in this country.

THE NEED FOR CIVILIAN AGENCY CONTROL

The key question during the hearings was: Should a military intelligence agency, NSA, or a civilian agency, NBS, be in charge of the government's computer standards program? The activities of NSA under both NSDD-145 and the Poindexter Directive in dealing with the private sector and the outrage expressed by the witnesses reinforced the view of the Committee and many others that NSA is the wrong agency to be put in charge of this important program.

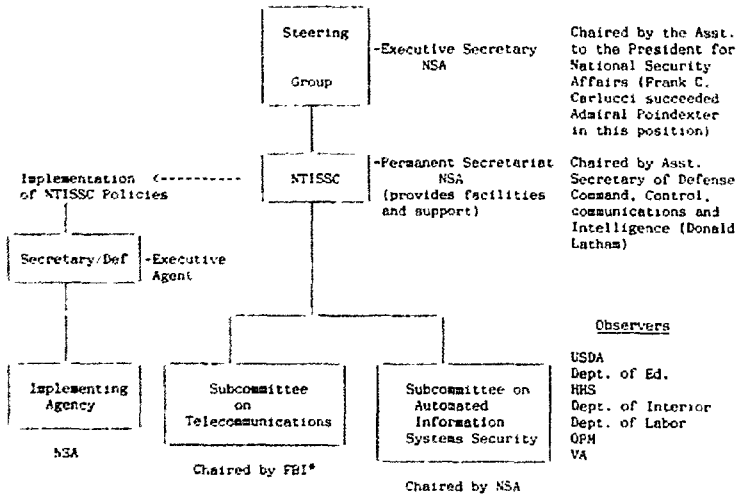
The National Security Agency

The National Security Agency (NSA), which was established by a secret presidential directive in 1952, has a lead role in implementing NSDD-145. Under that directive, NSA would act as the day-to-day manager of all computer security activities undertaken pursuant to the directive. In this regard, NSA would assess threats to sensitive systems and analyze the overall security posture of Federal agencies. NSA would also direct Federal agencies to provide the appropriate technology for the protection of automated information.

Although the Defense Department asserts that NSDD-145 management structure is well balanced between civilian agencies and the military, virtually all key positions are held by national security officials. For example, the Steering Group of the computer security committee is chaired by the National Security Advisor (Poindexter, Carlucci) and its executive secretary is NSA. The committee itself is chaired by DOD Assistant Secretary Donald Latham. NSA is the Permanent Secretariat and provides the facilities and support for the committee. The Secretary of Defense is responsible for implementing the policies issued by the committee which is done by NSA on a day-to-day basis. Without doubt, this committee is tightly controlled by DOD and NSA as is illustrated in the following chart.

[21] Statement of Congressman Glenn English, dated February 25, 1987.

27



Steering Group Membership

Secretary of State
Secretary of Treasury
Secretary of Defense
Attorney General
Director of OMB
Director of CIA

NTISSC Membership

Representatives of Steering Group PLUS
Secretary of Commerce
Secretary of Transportation
Secretary of Energy
Chairman, JCS
Administrator, GSA
Director, FBI

Director, FEMA
Chief of Staff, USA
Chief of Naval Operations
Chief of Staff, USAF
Commandant, USMC
Director, DIA
Director, NSA
Manager, National Communications System

* Although the Subcommittee is chaired by the FBI, communications security is one of NSA's main missions and, therefore, it plays a major role in the activities of the group.

The appropriateness of having NSA, a military intelligence agency, appointed as the computer security czar under NSDD-145 raises serious questions. First, the role assigned to NSA under NSDD-145 would require the diversion of a substantial amount of resources from its national security mission to overseeing the protection of unclassified information in the civilian agencies and the private sector. Second, NSA's (and DOD's) natural tendency to restrict and even deny access to information that it deems important would disqualify that agency from being put in charge of the protection of non-national security information in the view of many officials in the civilian agencies and the private sector. Finally, concern has been raised that giving NSA more authority to involve itself in the affairs of the civilian agencies and the private sector could involve that agency in domestic surveillance activities in violation of its charter.

The National Security Agency, since its establishment in 1952 by President Truman, has historically remained out of public view.[22] In fact, until 1962, NSA's existence was not even acknowledged in the U.S. Government manual. No director of NSA ever appeared before a Congressional committee in public session until 23 years after its creation—1975. The first press interview was not given until 1978.[23] The reason for this secrecy is its unique mission which is two-fold—signal intelligence (SIGINT) and communications security (COMSEC). SIGINT involves the monitoring of foreign communications to produce foreign intelligence. COMSEC involves the monitoring of official government communications to ensure that our own communications systems are secure from foreign interception and exploitation. To perform its mission, NSA is heavily dependent on the use of computers, particularly in the decryption of encoded messages. Its success is also heavily dependent on ensuring that the results of its work are maintained with the utmost secrecy. Thus, NSA has always maintained a low profile even to the point that its very existence was for many years kept from the American people.

NSA's secretiveness resulted in an inappropriate approach when it attempted to deal with national policy issues such as the issue of public cyrptography. Historically, this science has been the exclusive domain of government, and in this country it is one of NSA's primary missions. However, with the advent of modern computers and communications, there has been in recent years considerable interst in cryptography, particularly by the business community, which is interested in keeping its proprietary information from competitors. As a result of the emerging need to protect information, the academic community has done research work in the field. NSA has made numerous attempts to either stop such work or to make sure it has control over the work by funding it, pre-publication reviews or other methods.[24]

---

[22] NSA was created by a top secret memorandum from President Truman to the Secretaries of State and Defense on October 24, 1952.

[23] Interview with Science Magazine in October 1978 by then NSA Director Vice Admiral B.R. Inman.

[24] In January 1981, the Director of NSA even went so far as to write this Committee and complain that the Committee had not forwarded to NSA a copy of its investigative report, "The

Continued

In one example, a professor in the late 1970's at the University of Wisconsin developed a device that protects computers from penetration by unauthorized individuals. The professor, following normal practice, signed over patent rights to the Wisconsin Alumni Research Foundation, which applied for a patent in October 1977. Subsequently, a secrecy order was received from the Patent and Trademark Office stating that disclosure of the principles involved in the device "might" be detrimental to the national security.[25] Those knowledgeable about the device were ordered to say nothing or risk penalties as great as two years in prison and $10,000 fine. The secrecy order which was initiated by NSA did not say why the national security was involved, state how long the order would be in effect, or explain any methods of appeal. After a storm of public protest, the secrecy order was rescinded on June 15, 1978.[26]

Another controversy has again risen with NSA's announcement that it wants to use a new Data Encryption Standard (DES) algorithm beginning in January 1988.[27] In its testimony, the American Banking Association stated that, according to NSA, algorithms cannot be used by the financial industry as a replacement for DES nor used intentionally or placed in equipment for use by non-U.S. entities. Furthermore:

> The algorithms will be secret, rather than public, which will make them unacceptable in some foreign countries, even if the NSA would allow their use overseas. *NSA is considering the retention of control over encryption keys, which would result in an unacceptable transfer of responsibility for the security of our data to a government entity.* Those conditions may be appropriate for national defense-related security, but are clearly inappropriate for use in the financial industry.[28] (Emphasis added.)

Although NSA is widely respected for its foreign intelligence accomplishments, that agency has at times involved itself in activities outside the scope of its foreign intelligence and communication security mission. In effect, it has aimed its intelligence expertise at American citizens. NSA's involvement in these activities and its role under NSDD-145 were described by the American Civil Liberties Union during this Committee's hearings when it stated that:

> NSA operates outside the normal accountability channels which control other agencies of government. * * * No

---

Government's Classification of Private Ideas," *prior* to its issuance. As pointed out by Chairman Brooks in reply to NSA, Congress does not submit its reports to Executive Branch agencies for prereview. Furthermore, all the material contained in the report was obtained from opening hearings and the public record.

[25] The secrecy order was initiated by NSA. After a storm of public protest, the secrecy order was rescinded on June 15, 1978.

[26] Committee on Government Operations report entitled "The Government's Classification of Private Ideas," dated December 2, 1980.

[27] The DES specifies a method for encrypting 64-bit blocks of cipher (encrypted text) using a user-specified 56-bit key. It was originally devised by IBM over 10 years ago. Later, with NSA's assistance, it was established as a standard by NBS. Even though NBS certified and issued the encryption standard, NSA's involvement was viewed with suspicion. During considerable public debate, allegations were issued by the academic community and others that NSA's involvement in the DES resulted in a smaller key length than was needed. Ostensibly, NSA wanted a key length large enough to provide communications security, but small enough for NSA to be able to read the messages.

[28] Statement of the American Banking Association, dated February 25, 1987, p. 3-4.

Director of NSA appeared in open session of Congress until 1975—and then only to answer to a series of programs of illegal acquisition of international cables and "watchlisting" and interception of the communications of anti-war and civil rights activists. Because of the "States Secrets Privilege," civil suits against NSA for unauthorized surveillance routinely have been dismissed to protect its super-secret surveillance capabilities.

We do not believe that DOD or NSA or the intelligence community are appropriate agencies to control communications and computer security in the civilian or private sector. Their tendency is to keep secrets and they have amply demonstrated that they do not weigh privacy and open government in the balance or if they do, they always strike the balance in favor of secrecy.

Moreover, we do not believe foreign intelligence agencies should be monitoring or surveilling private companies in the United States to determine which companies or executives are taking "appropriate" security measures or disseminating public information to the "wrong" people or "No No" list.[29] Intelligence agencies may intimidate companies or have a "chilling effect" on their information dissemination practices. Companies will not want to be on a list or in a file of "uncooperative" companies who lack proper consideration for national security.[30]

Dr. David Kahn, a renowned expert on NSA, testified that under NSDD-145 NSA is currently involved in one program that may harm the nation more than it helps it. Kahn was referring to NSA's program to develop and certify only those scrambler devices (STU-III) [31] that is supplies. The witness noted that by not certifying those scrambler devices developed in the private sector, NSA was virtually compelling the private sector to use NSA's scramblers. Kahn noted that this presents the dangers of:

Big Brotherism. The N.S.A. intends to offer its STU-III (Secure Telephone Unit, Model III) to protect private-sector telephone conversations under the mandate of NSDD-145. Because of N.S.A.'s expertise, the STU-III will almost certainly be better than any other scrambler in the private sector. But the way in which it works will not be

[29] The National Aeronautics and Space Administration (NASA) established the so-called No-No list ostensibly to provide U.S. scientists with a head start in acquiring and using available information. It is a list of companies who are refused access to NASA's data bases because they export information. Unfortunately, those NASA officials who maintain this list have demonstrated little faith in the ability of the U.S. scientific community. The economic vitality and strength of this country is a direct function of the ability of the scientific community to acquire and use information more efficiently and effectively than other nations.

[30] Statement of the American Civil Liberties Union, dated February 25, 1987, pp. 23-25.

[31] The Washington Post, in an article dated March 6, 1987, reported that NSA secretly monitored Robert C. McFarlane and Admiral Poindexter, former National Security Advisors, and other White House officials when these individuals used their Secure Telephone Units (STU's). Those phones have computerized encryption devices which make the calls unintelligible to anyone attempting to listen in. NSA is the principal agency involved in the production and regulation of these phones. When questioned about this after the Committee's hearings, NSA responded that "NSA did not record or monitor Robert C. McFarlane or other top White House officials. Over one three-day period, NSA did monitor communications associated with a White House military office communications exercise. This was done at their request."

made public: the integrated-circuit chip that embodies the algorithm will be tamperproof. This leaves open the possibility that the cryptosystem will contain a "trapdoor" that will enable N.S.A. to break it.[32]

When Dr. Kahn asked an NSA official about this possibility, that official said that the public would have to trust NSA. On the issue of trust, Kahn noted that:

> The post-Watergate Congressional investigations of the intelligence agencies disclosed that N.S.A. had for years been intercepting private American cablegrams, radiograms, and telephone conversations and had enthusiastically participated in the notorious Huston plan, which would have invaded Americans' civil rights. So the N.S.A. can no longer expect that the public will place a blind confidence in its integrity. It must be subject to the same checks and balances as all other institutions of this government.[33]

Kahn also noted another danger of NSA involvement in private sector activities:

> Restraint of innovation in cryptography. If N.S.A. furnishes the equipment to be used under NSDD-145, private inventors will have less incentive to create, and private firms less incentive to produce, new cryptosystems. And the two most widely used cryptosystems of the past decade have come from private inventors. One is the Data Encryption Standard, devised by Horst Feistel while he was with I.B.M. It has conferred secrecy upon innumerable confidential transactions. The second is public-key, or asymmetric, cryptography. The concept was first proposed in the public literature in 1975 and realized in a workable form a year later. It has made possible all sorts of ingenious activities, such as authenticating telegraphic signatures and validating arms-control data while concealing secrets. No one knows whether these systems would have been invented if the N.S.A. program was in effect and had shrunk the potential market. But it is not an inconceivable situation.[34]

Among other things, Kahn recommended that the legislation being considered by the Committee should:

> (3) Abolish NSDD-145's "sensitive but unclassified" category and deny the Department of Defense any control over unclassified communications.
>
> (4) Require some nonmilitary agency, as perhaps the National Bureau of Standards or the Federal Communications Commission, to encourage and assist private organi-

---

[32] Statement of David Kahn, dated February 25, 1987. Dr. David Kahn is the author of the book, "The Codebreakers," the Macmillan Company, 1967.

[33] Kahn also noted that "the danger of total government control in this field is made concrete by a singular case: N.S.A. and/or its British counterpart invented asymmetric cryptography some years before the private sector but kept it under wraps. Thus the government deprived the public of this system's many advantages for some time. Such a condition is likely to be aggravated under the N.S.A. program's restrictive arrangement."

[34] Statement of Dr. David Kahn, dated February 25, 1987.

zations to encrypt information that might aid another country.

(5) Require that the cryptosystems used in encrypting this nongovernmental information be nonsecret (the secrecy to reside in the keys) and certified as secure by the National Bureau of Standards with the assistance of the National Security Agency.[35]

An example of the dangers that could be involved as a result of NSA's domestic activities surfaced almost two years ago when it was publicly revealed that the agency was investigating the computer program that counted more than one-third of all the votes cast in the United States.[36] Ostensibly, NSA was performing this investigation under the authorities assigned to it by NSDD-145 in order to determine whether the computer system was vulnerable to fraudulent manipulation. As part of its work on this system, the agency gained detailed knowledge into the functioning of the computer program and any inherent weaknesses within the system that could be tampered with. The central focus of NSA's investigation was the vote-counting program of Computer Election Systems of Berkeley, California, which is apparently the dominant company in the manufacture and sale of computer voting apparatus. According to the New York Times, the company's program and related equipment was used in more than 1,000 county and local jurisdictions to collect and count 34.4 million of the 93.7 million votes cast in the United States.

In this particular case, the Committee does not suggest that what NSA attempted to do was illegal or done with any malice. The question is whether it is proper for a military intelligence agency that has no charter for domestic intelligence to involve itself in activities within the United States, particularly our country's election process.

APPROPRIATENESS OF NSA WORK TO CIVILIAN APPLICATIONS

"Technical Guidelines"

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.[37] 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 Bureau

---

[35] *Ibid.*

[36] Burnham, David, "U.S. Examines If Computer Used in '84 Election Is Open to Fraud," New York Times, September 24, 1985, p. A-17.

[37] In the 99th Congress, NSA also attempted to prevent the passage of H.R. 2889. On December 22, 1986, one of the subcommittees created by NSDD-145 and chaired by NSA reported to Latham on its accomplishments during 1986. It stated "Provided staff support for lobbying effort that successfully blocked H.R. 2889 from passage by the 99th Congress." However, lobbying against legislation by Federal officials is against the law. The Anti-Lobbying Act, 18 U.S.C. 1913, prohibits the use of appropriated funds to be used for financial activities aimed at influencing the outcome of legislation. The DOD Inspector General is now investigating the lobbying activities of DOD and NSA officials both last Congress and this Congress.

of Standards.[38] 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. NSA, on the other hand, is unfamiliar with it.[39] Further, NSA's products may not be useful to the 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.

Disclosure vs. Integrity

While NSA does have a computer center and millions of dollars in funding, its claim that it is the olny agency with the expertise to develop standards is highly questionable. Testimony received during the hearings which criticized the use of NSA's products for civilian use. For example, the only product of recognition that NSA has produced is the Orange Cook (the Trusted Computer System Evaluation Criteria). This book may be good for the military agencies, but is of little value to civilian agencies. This is because NSA's approach to computer security is to prevent disclosure of information while the civilian sector is interested in maintaining the integrity of information, i.e. ensuring that payroll records are not changed to give an employee a higher paycheck.

According to Robert H. Courtney, a private sector consultant on computer security.

> The Computer Security Center at Fort Meade has been in place for about five years. I believe that no Federal agency has gained a truly meaningful and material enhancement in its computer security posture as a consequence of the contributions of that center. *Their guidance*

[38] The protection of computer and communications is generally regarded as involving three approaches—physical, administrative, and technical. Physical security involves the protection of a computer facility from outside penetration and involves combination locks on doors, fences, and so forth. Administrative security measures are operating instructions issued by an agency involving security procedures to be followed by agency personnel, such as which employees are allowed into a computer room. Technical security involves developing software measures to prevent a malicious intruder form unauthorized access or manipulation of vital information—even to the extent of taking control of the operating system or other software. It also involves the protection of hardware such as ensuring the components of a computer system have not been altered by an outside party. Similarly, the transmission of information over communications lined needs to be protected from someone surreptitiously "tapping" into the line and accessing the information for their own purposes.

[39] An example of the inappro priateness of NSA standards is shown by NSA's proposal that our nation's banking system use a new Data Encryption Standard (DES). At our hearings, testimony was received that showed the bankers were very concerned about this proposal for NSA. If required to use NSA's new algorithm, the witness noted that it would be disruptive and very expensive since many of the banks had in the last few years just bought and installed the earlier DES issued by the NBS. The banks objected to being at the mercy of one agency which would change algorithms at any time in the future. Similarly, the banks did not feel "comfortable" with NSA holding all of the keys to the new cryptosystem, thereby giving NSA the ability to read all information passed over the banks communications lines.

is not even accepted by the major data processing operations within NSA.

The National Computer Security Center (NCSC) has not been able to make an important contribution to computer security for several reasons. An understanding of these reasons is essential to full appreciation of the importance of H.R. 145.

The NCSC is imbedded deep within the intelligence community. The problems to which they have given almost exclusive priority reflect the classic and often limited data security concerns of that community. They have repeatedly demonstrated their inability to understand the computer security problems of organizations other than those directed by the Assistant Secretary of Defense for C³I to whom they report. For this reason, *the principal thrust of their efforts had been directed at the security of not more than 8% of the DOD data processing capacity and almost none of that of the civil agencies of government.*

The NCSC people have spent more time trying to convince other agencies that their security problems are the same as those of the intelligence community than they have spent trying to understand the problems of those other agencies. . . . no concern was shown for the well-being of the agencies whose security programs would be warped to satisfy NSA's goals.[40]

Further, we rarely see within DOD adequate appreciation of the need to protect data against illicit modification, whether it be accidental or intentional, as opposed to the problem of disclosure. I am convinced that persons whose loyalty and honesty are beyond question but whose judgement and competence and willingness to be both careful and diligent leave much to be desired can easily do as much harm as can others who would disclose classified data. Our security concerns must embrace modification, destruction, and delay in the availability of data as well as the problem of unauthorized disclosure on which the NCSC converges its attention.

---

[40] courtney further noted that "I see consistent neglect by DOD of extremely important, readily correctable security progblems simply because of their unfortunate orientation toward the protection of only those data which are classified. Navy Supply affords an excellent example.

"The Navy's operational capability can be seriously impaired by the destruction or malicious modification of the data on which its logistic support is based. Materiel in the correct amount when and where it is supposed to be is essential to the proper conduct of so vast a supply operation. Much classified data can be disclosed with less damaging consequences than would illicit modification or destruction of data showing location, quantity, and shipping information of vital supplies. Yet, even today, NAVSUP is heavily dependent upon the loyalty and good will of hundreds of uncleared clerical folks contributing and modifying data in NAVSUP systems which do not incorporate even the most elementa' security measures commonly encountered in U.S. industry.

"The movement of our ships and, most particularly, the arrivals and departures of our submarines are readily determinable from an examination of data in unsecured systems to which access is not constrained to only those persons who need those data to get their respective jobs done. The dates by which materiel must reach the ports for loading onto specific ships offers excellent guidance to those who want to know about the departures and arrivals of our naval forces in specific ports. Those are available to many people who do not need them. Equally important, accesses by those who do need them are rarely recorded so as to hold those people fully accountable for adequate discretion in the use of those data and for their proper safeguarding."

It is important that those developing security measures for Federal agencies understand that the security problems of many agencies more closely resemble those of J.C. Penneys than they do those in C³I.[41] (Emphasis added.)

Further, NSA tends to provide the highest level of protection (the most expensive) for its information, while the civilian sector evaluates the importance of the information it wants to protect and assigns a level of protection that is warranted. For example, Federal tax records would most likely require administrative, physical, and technical protection, while library data bases would only require physical and administrative measures to protect the actual computer facility itself.

The American Banking Association witness made this point in her testimony before the Committee when she stated:

> The first issue of concern is the move to protect all sensitive information in the same manner—business information, information of importance to the national interest, and classified defense information. *Within both the public and private sectors, there is a need for a broad spectrum of information systems security standards, techniques, and tools. There must be a range of security "solutions" that can be matched to the value of the information being protected, and the nature of the threats.* Outside of the classified and national security arenas, both the private and public sectors must select cost-effective security measures.
>
> To use a simple analogy, to travel from Point A to Point B one could choose a motorcycle, a truck, or a tank. These vehicles vary widely in cost, and each is best suited to a different environment. *Under NSDD-145 and the programs that have resulted from that directive, the range of computer security solutions being developed have been narrowly focused on the "tank" end of the spectrum.* The danger in doing this is, the road to be traveled might not accommodate a tank, or the traveler might not be able to afford the price tag. Thus, the trip might not be taken at all.[42] (Emphasis added.)

Allegations were also made to the Committee that having both NBS and NSA working on computer security standards would hamper efforts to develop secure systems that would be able to handle both classified and unclassified information. This is a reference to work being done on multi-level security. In fact, the Defense Department, including NSA, has been working on this problem since the early 1970's with limited success and there is no indication that a major breakthrough is possible in the foreseeable future.

Another assertion made to the Committee is that it would be wasteful and inefficient to have both NBS and NSA developing technical standards. This is simply not true. As noted earlier, the requirements of the civilian agencies are different than that of the

[41] Statement of Robert H. Courtney, dated February 25, 1987.
[42] Statement of the American Banking Association, February 25, 1987.

military, i.e. protecting the integrity of information versus the disclosure of information. Therefore, having NBS in charge of the computer standards within the civilian agencies and interacting with the private sector would not be wasteful or inefficient.

Robert Courtney perhaps summed it up best when he noted that:

> *The thoroughly introverted approach taken by the NCSC is far too wasteful for us to suffer its continuation.* The prompt passage of H.R. 145 is a wholly necessary if not sufficient condition to the development of appropriate safeguards for federal data and the education of those in the respective agencies who must select and apply them. The funding level of the NBS computer security activity must be increased significantly but their increase should not be near so great as the appropriate decrease in the budget of the current Computer Security Center if it reverts, as it should, to being the DOD Computer Security Center.
>
> *There should be no concern that the operation of two centers of competence in computer security might be wasteful. There is sufficient difference between the problems which would be addressed by the DOD center and those which would be treated by the NBS operation to assure little duplication of effort.*[43]

PROTECTION VS. ACCESS

The world is now in a period some refer to as the information age. During our lifetimes, the rapid advances in the ability to collect, process, and disseminate information have had as far-reaching an effect on our world as the industrial revolution had on the world of our forebears. Unfortunately, there are those who fear this change. They believe the unbridled development and use of new technologies will lead us into uncertain ventures. As a result, some would turn their backs on America's commitment to innovation and progress and cloak many of our advances in secrecy and deny access to them by a large portion of our population. This fear should not be allowed to stifle our future. The challenge facing our government and our people is to strike a balance between the need to protect national security and the need to pursue the promise that the intellectual genius of America offers us. H.R. 145 was developed in large part to ensure that this delicate balance is maintained and to respond to those in the national security establishment who have lost signt of this important principle.

Furthermore, one of the benefits of a full and open society is the rich exchange of ideas and knowledge unfettered by governmental intervention and redtape. The successes of our scientific, technical, and medical communities have been based upon the free exchange of data and information. 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. There are other practical problems as well. First, DOD does not have the resources

[43] Statement of Robert H. Courtney, dated February 25, 1987.

to classify and control all of the information that would be encompassed by NSDD-145 and the Poindexter Directive. Second, the cost of applying DOD-type security measures to civilian agency and private sector information systems would be overwhelming. In addition, DOD has its hands full trying to even modestly protect its own classified information and it would be foolhardy to expand its jurisdiction to protect the unclassified information contained in the civilian agencies and the private sector.

In order to ensure that the Computer Security Act is designed to protect and *not* to restrict access to government information, specific provisions were added to H.R. 145 (Section 8) which make it explicitly clear that the Computer Security Act has no bearing on the public availability or use of information. The designation of information as sensitive under the Computer Security Act is not a determination that the information is not subject to public disclosure nor does such a designation bear on the determination to disclose. Information that requires protection while it is being transmitted over telecommunications facilities or while it is being stored in a computer may nevertheless be public information under the Freedom of Information Act (FOIA) or other statutes or regulations. The protection may be necessary in order to prevent unauthorized use of a computer system or to prevent the information from being altered in an unauthorized manner.

H.R. 145 is strictly neutral with respect to public disclosure of information. Any information that was required to be disclosed under the Freedom of Information Act or other laws before enactment of the Computer Security Act will still have to be disclosed after enactment. Requests for information that was previously subject to withholding and that continues to qualify for withholding may be denied.

In addition, the language of the bill makes it explicit that the Computer Security Act cannot be relied upon by an agency to modify, limit, restrict, or otherwise affect the use or redisclosure of information that has been released under the FOIA. Once information has been released, the requester remains free to use the information in the same fashion that was permitted before the Computer Security Act was passed. Information that is released under the FOIA remains beyond restriction by an agency.

Another purpose of Section 8 is to prevent any provision of the Computer Security Act from being construed to authorize any Federal agency to exercise any control over privately-owned information, public domain information, or information disclosable under the FOIA or other laws. As noted earlier in this report, efforts were made by CIA, FBI, NSA and other Federal officials to restrict or monitor the use of unclassified, private sector computerized data bases such as LEXIS and NEXIS. This section makes it explicitly clear that no such authority is granted to Federal agencies by the Computer Security Act.

Further, Section 8 provides that this limitation on construction of the Act applies regardless of the medium in which information is stored. Thus, where the government is without authority to restrict or regulate the content or use of information that appears in newspapers, the government remains without such authority with respect to the same information that is maintained on microfiche,

computerized data base, optical disk, or other computer system storage medium.

The problem of government control over computerized information has already been recognized by this Committee. Earlier Committee reports have pointed out the dangers when agencies attempt to restrict private use of computerized data bases. See generally *Electronic Collection and Dissemination of Information by Federal Agencies: A Policy Overview,* House Report 99-560 (1986). In particular, this report criticizes the decision by the National Library of Medicine (NLM) to place redisclosure restrictions on the data tapes used to suppoort the Medlars (Medical Literature Analysis and Retrieval System). Although the data base is not copyrighted and is unrestricted in its printed version, NLM controls use of the data tapes through a questionable licensing arrangement.

The National Library of Medicine justifies the Medlars restrictions on the basis of a ruling in a 1976 Freedom of Information Act case.[44] However, the decision in that case has been found by this Committee to be incorrect as a matter of law and as a matter of policy. The Committee continues to believe that information restrictions such as those imposed by NLM further no valid government purpose and might be used to prevent use of data that may be uncomplimentary, censor information, or hide documents.[45]

Section 8 of the Computer Security Act is intended to ensure that nothing in the Act will be construed as favoring, supporting, justifying, or extending such information restrictions over privately-owned information, over unclassified government information that is available to the public through the FOIA or other law, or other public domain information.

OTHER MATTERS

National Security Decision Directives—Secret Law

During the Committee's review of the improprieties carried out by DOD and NSA under the auspices of NSDD-145, it was learned that this directive was only the tip of the iceberg. Other NSDDs were also found to exist. Most disturbing was the fact that not even Congress has had a chance to review most of these directives. During the hearings, Congressman Anthony C. Beilenson, Chairman of the Oversight and Evaluation Subcommittee of the House Permanent Select Committee on Intelligence, testified that even the Intelligence Committee has not had access to the directive and, therefore, does not know how many have been issued or what subjects they may cover.

The Congressional Research Service (CRS) was asked by the Committee to review the use of NSDDs by this Administration. CRS reported to the Committee that since 1981 over 200 such directives had been issued and that only 5 had been publicly disclosed.[46]

---

[44] *SDC* v. *Matthews*, 542 F.2d 1116 (9th Cir. 1976).

[45] The Committee also criticized the holding of *SDC* v. *Matthews* in the report accompanying H.R. 4862 (99th Congress), the Freedom of Information Act Amendments of 1986, House Report 99-832 at n.1 (1986).

[46] Information from published documents suggest that at least 260 NSDDs have been issued over the last six years.

The rest remain under security classification and Congress and its committees have not been given acccess to these documents.

According to CRS, the NSDDs comprise an on-going system of declared U.S. policy statements and are, with rare exception, secret policy instruments, maintained in a security classified status. Even in those instances when they are available to the public, the directives are not published in the Federal Register and must be requested in writing.

The CRS testified that the directives seem to be expanding into even more diverse and varied areas than was true in the past. For example, NSDD-84 prescribed conditions for the use of classified information by Executive Branch personnel. NSDD-145 establishes national policy for telecommunications and automated information systems security. NSDD-189 involves the establishment of a scientific, technical, and engineering information transfer policy. NSDD-196 concerns counterintelligence matters, and NSDD-197 addresses the reporting of agency contracts with foreign nationals from countries hostile to the United States.

CRS also noted that:

> . . . press accounts have reported that NSDDs have been used in providing aid to Contra forces in Latin America and authorizing $50 million for Argentina to train Contra guerrillas, as well as to inaugurate a disinformation campaign against Libya to give the impression that a U.S. attack was imminent and to set U.S. policy that a quote, "regime change," unquote, was sought in Libya.
>
> One of the most interesting press disclosures in this regard was in the March 8, 1987, Philadelphia Inquirer. It was a front-page story which [was] captioned—the opening paragraph began this way: "President Reagan in 1984 authorized an ultrasecret U.S. counterterrorism unit whose leaders included retired Air Force Major General Richard B. Secord. It was intended to bypass normal governmental controls, according to interviews and recent government investigations." The authorization of that particular unit was through an NSDD, so the *Inquirer* reported.
>
> *National Security Decision Directives clearly pose a problem for a free and open society and bring the U.S. and bring all of us very close to one of the most dangerous conditions of authoritarian or totalitarian government, rule by secret law.*[47]

As Chairman Brooks stated during the hearings:

> We must . . . take a close look at how national security decision directives are issued and implemented. From what little we know of the process, it appears there is a great potential for the abuse of power that we have witnessed under NSDD-145.
>
> In my view, it is about time Congress demanded access to all these directives. We need to find out what has been going on in the government [over the last six years].[48]

---

[47] Hearing transcript, March 17, 1987, pp. 98-99.
[48] Hearing transcript, March 17, 1987, p. 5.

Implementation of policy decisions through the issuance of undisclosed directives poses a significant threat to Congress' ability to discharge its legislative and oversight responsibilities under the Constitution. Operational activities undertaken beyond the purview of the Congress foster a grave risk of the creation of an unaccountable shadow government—a development that would be inconsistent with the principles underlying our republic.

Export controls

In its zeal to restrict access to computerized data bases, the military intelligence agencies, led by NSA, paid little heed to other aspects of our country's national interests, particularly its economic welfare. With the balance of trade deficit reaching unprecedented proportions, the military has been able only to fucus on who is accessing our unclassifeid data bases, not on the economic benefits that this new and vital industry is providing to this country, such as an annual trade surplus of $1 billion.

Ken Allen, Senior Vice President of the Information Industry Association (IIA), in an interview with Federal Computer Week, noted that "The on-line data base industry is one of the few places where there is a positive balance of trade. But now, in England and Australia in particular, editorials have been written that say: Don't depend on the Americans for information. At any moment their government may declare it sensitive."[49]

Jack Biddle, President of the Computer and Communications Industry Association (CCIA), testified that DOD's insistence on overly restrictive export controls has had a devastating effect on the computer and communications industry. Biddle stated that our industry:

> . . . has had some experience with DOD over the past decade with respect to export controls which has been pretty devastating to the industry. We have seen a level of paranoia develop in DOD to where it's almost literally reached the point where they would bar the export of paperclips because a terrorist might straighten one out and stick somebody in the eye with it.
>
> We are losing our world leadership in computer technology, because we are forfeiting our overseas markets because of DOD's fear that a blue box might slip through the Iron Curtain.
>
> Then we see NSDD-145. And with that background of DOD paranoia clearly in our minds, it's rather frightening, because we can foresee the possibility that our scientists will not be able to communicate with each other to maintain a leading edge in technology, while the Japanese scientists will be conversing with each other in open forums.
>
> One has to wonder, at what point do we give up our freedoms in order to coexist in the world with a country that has no freedoms? And it would appear increasingly that DOD's view of this is that we must reach parity by adopting the styles and policies of our adversaries.[50]

[49] Federal Computer Week, May 4, 1987, p. 3-4.
[50] Hearing transcript, February 26, 1987, p. 106-107.

The National Academy of Sciences in a recent report showed that efforts to keep the Soviets from acquiring high technology from this country have cost the U.S. 188,000 in lost jobs and $9.3 billion a year. According to the report:

> A reasonable estimate of the direct, short-run economic costs to the U.S. economy associated with U.S. export controls was on the order of $9.3 billion in 1985. This is a very conservative estimate because it does not cover all aspects of economic costs and it only applies to a subset of the potential scope of business activity influenced by U.S. export controls . . . . Associated just with lost U.S. exports was a reduction in U.S. employment of 188,000 jobs. If we were to calculate the overall impact on the aggregate U.S. economy of the value of lost export sales and the reduced R&D effort, the associated loss for the U.S. 1985 GNP would be $17.1 billion.[51]

Furthermore, export controls work when the U.S. is the only country with that technology, otherwise the Soviet bloc countries will obtain the technology from our allies who are more than willing to sell to the Soviet Union. The report stressed that the economic vitality of the United States is dependent upon overseas trade. U.S. dominance in high technology has been eroded by Japan, Western Europe and the newly industrialized nations of Asia and the Pacific. Until 1981, a vigorous U.S. high-technology trade surplus helped offset deficits in other sectors, but that surplus decreased to the point where high technology trade became a deficit last year. In commenting on the competitive effects of export controls, the report cited a survey of private sector companies which follows:

COMPETITIVE EFFECTS OF CONTROLS

> The panel's survey respondents,[52] reflecting on their experience over the 12 months prior to May 1986, perceived the control system as frequently having significant adverse effects on their business:
>
> 52 percent reported lost sales primarily as a consequence of export controls;
>
> 26 percent had business deals turned down by Free World customers (in more than 212 separate instances) because of controls.
>
> 38 percent had existing customers actually express a preference to shift to non-U.S. sources of supply to avoid entanglement in U.S. controls; and
>
> more than half expected the number of such occurrences to increase over the next 2 years." [53]

The NAS report was done by a committee of eminent former defense officials, business executives, and academics which included

[51] Balancing the National Interest, National Academy of Science, p. 264.

[52] The sample of companies surveyed was oriented toward firms in the electronics (equipment and components), aircraft, (airframes, engines, and parts), instrumentation, and machine tool sectors. The 170 respondents accounted for roughly $36 billion of foreign sales in 1985, or approximately 28 percent of estimated total U.S. high-technology sales.

[53] Balancing the National Interest, National Academy of Sciences, 1987, p. 116.

former National Security Agency Director and Air Force Chief of Staff, General Lew Allen, Jr. (who chaired the Committee); former Defense Secretary Melvin Laird; and former Director of the National Security Agency and Deputy Director of the Central Intelligence Agency, Admiral Bobby Ray Inman. Clearly, the assessment by these former high level government officials that restrictive export controls have harmed our national interests rather than helped it underscores the necessity of greatly relaxing these controls. This could include removing DOD from its current position of vetoing technology sales overseas. Its role should be relegated to providing advice on the need for specific controls. In regard to the development of computer standards and guidelines, the Committee would expect the Secretary of Commerce to ensure that such standards would be implemented so as to not negatively affect trade with the other countries.

The National Security Advisor

On February 25, 1987, the Legislation and National Security Subcommittee unanimously voted to subpoena Admiral Poindexter, former National Security Advisor, and his aide, Kenneth de Graffenreid, when they failed to appear voluntarily to discuss their role in the issuance of the two computer security directives: National Security Decision Directive (NSDD) 145, signed by President Reagan in September of 1984, and a subsequent directive issued over the personal signature of Admiral Poindexter last October.

These individuals played key roles in drafting NSDD–145 and convincing the President to sign the document in September of 1984. This Directive gave the national security agencies the authority to control public access to unclassified information located in civilian agencies and even the private sector.

Furthermore, on October 29, 1986, Admiral Poindexter issued, under his own signature, a directive which further expanded DOD's control to a wide spectrum of scientific, economic and cultural information in our nation. This document made no pretense of being an advisory document to the President and there was no indication that the President even knew about it. This Directive is an operational order demanding that all agencies of the Federal Government take certain actions.

While Congress has traditionally respected the privilege of confidentiality between the President and his closest advisors, it cannot allow these officials to use this privilege as a shield—they must be held accountable for their actions as any other public official when they take on an operational role in directing Executive Branch activities.

As Chairman Brooks noted during the hearings, "The basement of the White House and the back rooms of the Pentagon are not places in which national policy should be developed. This issue should be debated and fully aired in public hearings. In my view, it is critical that Congress reestablish civilian control over the Federal computer security program. We must also rein in those national security officials who have used the program as a means to implement a new form of government censorship. It is time to reaffirm the principle of the free and open flow of information in this country."

THE ADMINISTRATION: NBS WILL BE IN CHARGE

As a result of the Committee's investigation into the censorship activities of the military intelligence agencies, White House and other high level officials began an intensive review of NSDD-145, the Poindexter Directive and the pending legislation on computer security. This review resulted in a series of letters sent to the Chairman of the Committee in 1987:

February 26. James C. Miller III, Director of OMB. Told the Committee that he was interested in working with the Committee on the bill and would shortly forward the Administration's views on H.R. 145.

March 12. Frank Carlucci, who succeeded Admiral Poindexter as National Security Advisor, notified the Committee that the concerns raised regarding NSDD-145 and the Poindexter Directive were "legitimate and important." Carlucci then said he was rescinding the Poindexter Directive and promised to review immediately NSDD-145, particularly the role of the National Security Advisor under that Directive.

March 16. Howard Baker, who succeeded Donald Regan as Chief of Staff to the President, wrote the Committee that (1) Frank Carlucci had rescinded the Poindexter Directive and was moving promptly to review NSDD-145, (2) the Administration will propose certain changes to H.R. 145, and (3) offered to furnish appropriate witnesses for the Committee's hearings to be held the next day.

March 17. Frank Carlucci sent another letter to the Committee reiterating the actions that had been taken regarding NSDD-145 and the Poindexter Directive. He also noted that an intensive interagency review of H.R. 145 had been initiated in order to arrive at an Administration position on the bill. Further, the White House was making available Secretary of Commerce Malcolm Baldrige and Deputy Secretary of Defense William Taft to present the views of the Administration on this issue. During the hearings, Deputy Defense Secretary Taft stated that *"The thrust of H.R. 145 is to give the principal responsibility in that area to the National Bureau of Standards. This would put a definitely civilian agency in the framework as the point for these decisions. We support that thrust. We think that that's a good thing and we would have the National Bureau of Standards play that role."* (Emphasis Added)

March 17. William R. Graham, the Science Advisor to the President, noting the critical nature of the lelgislation, reiterated that an inter-agency review had been initiated on the bill. Further, OMB has taken the lead in the review and would provide the Administration's position on the bill to the Committee.

On May 12, OMB Director James C. Miller III, sent the following letter to the Committee:

EXECUTIVE OFFICE OF THE PRESIDENT,
OFFICE OF MANAGEMENT AND BUDGET,
Washington, DC, May 12, 1987.

Hon. JACK BROOKS,
Chairman, Committee on Government Operations,
House of Representatives, Washington, DC

DEAR MR. CHAIRMAN: I am pleased that through intensive consultations between the Administration and the Congress great progress has been made toward agreement on a Computer Security Act of 1987. I hope that this statement of Administration views will assist in offering constructive solutions to areas where further improvements are desirable.

As we have reviewed H.R. 145, a primary concern has been to assure that the roles as the National Bureau of Standards (NBS) and the National Security Agency (NSA) are discharged in a manner that will promote a sound public policy and result in efficient, cost effective, and productive solutions. In this regard it is the Administration's position that NBS, in developing Federal standards for the security of computers, shall draw upon technical security guidelines developed by NSA in so far as they are available and consistent with the requirements of civil departments and agencies to protect data processed in their systems. When developing technical security guidelines, NSA will consult with NBS to determine how its efforts can best support such requirements. We believe this would avoid costly duplication of effort.

Computer security standards, like other computer standards, will be developed in accordance with established NBS procedures. In this regard the technical security guidelines provided by NSA to NBS will be treated as advisory and subject to appropriate NBS review. In cases where civil agency needs will best be served by standards that are not consistent with NSA technical guidelines, the Secretary of Commerce will have authority to issue standards that best satisfy the agencies' needs. At the same time agencies will retain the option to ask for Presidential review of standards issued by the Department of Commerce which do not appear to be consistent with U.S. public interest, including that of our national security. I am enclosing proposed changes to the present text of H.R. 145 which are consistent with the NBS-NSA relationship outlined above and make several minor changes that would further improve the bill.

In closing, I want to assure you that a reported bill within the parameters outlined in this letter will have the Administration's support.

Sincerely yours,

JAMES C. MILLER, III,
Director.

CONCLUSION

The Committee believes that H.R. 145 provides the necessary legislative authority for the government to initiate and implement a strong and viable computer security program which will benefit both Federal agencies and the private sector. There is no question that such a program is urgently needed. Too much information and

data (personal, economic, financial) is being left unprotected in our government's computer and communications systems. Adequate protection must be provided to these systems, and H.R. 145 provides the right measures in terms of training, awareness, research and standards to accomplish this important goal.

H.R. 145 also provides a statutory base for NBS to take the government-wide lead in developing a useful and viable computer-security program. Clearly, it is NBS that should spearhead the government's computer security initiatives and be the focal point for (1) implementing these initiatives in the civilian agencies, (2) liaison with the private sector, and (3) representing the interests of the international arena. Further, H.R. 145 recognizes, as a practical matter, the resources of NSA and allows that intelligence agency to continue its traditional role of providing computer security for critical defense missions. The bill also provides a statutory base for NSA to assist NBS in the furtherance of its mission.

Section-by-Section Analysis

Section 1. Short title

Section 1 titles the Act as the "Computer Security Act of 1987."

Section 2. Purpose

Subsection 2(a) affirms that it is the intent of Congress that improving the security and privacy of sensitive information in Federal computer systems is in the public interest and thereby creates a means for establishing minimum acceptable security practices for these systems.

Subsection 2(b) states the following specific purposes of the bill:

—by amending the Act of March 3, 1901, to assign to the National Bureau of Standards (NBS) the responsibility for developing standards and guidelines for Federal computer systems. This includes the responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems. NBS may seek the advice and technical assistance of the National Security Agency (NSA) if NBS believes it would be appropriate to do so.

—by amending section 111(d) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759), to provide for the promulgation of standards and guidelines developed by NBS by the Secretary of Commerce.

—to require the establishment of security plans by all operators of Federal computer systems that contain sensitive information, and to require the mandatory periodic training of all persons involved in the management, use or operation of Federal computer systems that contain sensitive information.

Section 3. Establishment of Computer Standards Program

Section 3 amends the Act of March 3, 1901 (15 U.S.C. 271-278h), by redesignating Section 18 as Section 20 and adding new Sections 18, 19, and 21.

Subsection 18(a) assigns to NBS the mission of developing standards, guidelines, and associated methods and techniques for com-

puter systems. This includes the development of uniform standards and guidelines for Federal computer systems. NBS would also have the responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems. This subsection also defines those systems which are excluded from the standards and guidelines developed by NBS.

This subsection also reaffirms that the primary purpose of the computer security standards and guidelines developed by NBS shall be to control the loss and unauthorized modification or disclosure of sensitive information maintained in Federal computer systems and to prevent computer-related fraud and misuse. Further, NBS shall submit its standards and guidelines (including recommendations as to whether they should be made compulsory and binding) to the Secretary of Commerce for promulgation under Section 111(d) of the Federal Property and Administrative Services Act of 1949. Finally, this subsection requires NBS to develop (1) guidelines for use by Federal computer system operators for training employees in security awareness and (2) validation procedures under which NBS can evaluate the effectiveness of computer standards and guidelines, including those related to security of computer systems.

Subsection 18(b) authorizes NBS (1) to assist the private sector, upon request, in using and applying computer standards and guidelines (2) to make recommendations to the Administrator of the General Services Administration (GSA) on policies and regulations proposed pursuant to Section 111(d) of the Federal Property and Administrative Services Act of 1949, (3) to provide technical assistance in implementing standards and guidelines to operators of Federal computer systems, (4) to assist the Office of Personel Management in the development of appropriate training regulations, (5) to perform research and to conduct studies to determine the nature and extent of vulnerabilities and to devise techniques for the cost-effective security and privacy of sensitive information in Federal computer systems, and (6) to coordinate closely with other Federal agencies to ensure maximum use of pertinent computer security measures and to ensure that standards and guidelines are consistent government-wide.

Subsection 18(c) authorizes the NBS to draw upon the computer system technical security guidelines developed by the National Security Agency to the extent that the National Bureau of Standards determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

Subsection 18(d) defines the terms "computer system", "Federal computer system", "operator of a Federal computer system", "sensitive information" and "Federal agency".

Subsection 19(a) establishes an Advisory Board within the Department of Commerce consisting of 12 members and a chairman, all appointed by the Secretary of Commerce. Four will be from the computer and communications industry, including producers of that industry. Four will be from outside the Federal Government and will also be expert in computer or telecommunications technol-

ogy (or related disciplines), but not employed by the computer or communications industry. Four will be from the Federal Government, with, at least, one being from NSA. The purpose of the Board is to ensure that NBS has direct input from those parties interested in the development of computer security standards.

Subsection 19(b) describes the duties of the Advisory Board, which include the identification of relevant issues and keeping NBS, the Secretary of Commerce, the Director of OMB, the Director of NSA, and the appropriate committees of Congress informed of these issues.

Subsection 19(c) describes the term of office of each member of the Board.

Subsection 19(d) requires a quorum of seven Board members before any action is taken.

Subsection 19(e) allows for travel expenses to be paid for non-government employees.

Subsection 19(f) allows the Board to use personnel from NBS or other agencies to accomplish its mission.

Subsection 19(g) clarifies the terms "computer system" and "Federal computer system".

Subsection 21 names the Act of March 3, 1901, as the National Bureau of Standards Act.

Section 4. Amendment to Brooks Act

Section 4 amends Section 111(d) of the Federal Property and Administrative Services Act of 1949.

Subsection d(1) requires the Secretary of Commerce to issue standards and guidelines pertaining to Federal computer systems which are developed by NBS. In order to improve the efficiency of operations or security and privacy of Federal computer systems, the Secretary can make such standards compulsory and binding. This subsection also incorporates a Presidential review of the standards and guidelines issued by the Secretary of Commerce. If the President determines that it is in the public interest to do so, he may disapprove or modify the standards or guidelines and direct the Secretary of Commerce to take the appropriate action. This authority to disapprove or modify standards or guidelines may not be delegated by the President and notice of such action must be transimitted to the appropriate committees of Congress and published in the Federal Register.

Subsection d(2) allows the head of a Federal agency to employ standards that are more stringent than those issued by the Secretary of Commerce if those standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary.

Subsection d(3) allows the Secretary of Commerce to waive compulsory and binding standards if the Secretary determines that compliance would have an adverse impact on the mission of an operator of a Federal computer system or cause a major adverse financial impact on the operator which is not offset by government-wide savings. The Secretary of Commerce may delegate waiver authority to the head of an agency, but further redelegation can only be made to the agency's senior official designated pursuant to the Paperwork Reduction Act, as amended. Notice of such waiver or re-

delegation must be promptly sent to the appropriate committees of Congress and published in the Federal Register.

Subsection d(4) requires the GSA Administrator to revise appropriate Federal Information Resources Management Regulations to be consistent with the standards and guidelines issued by Secretary of Commerce.

Subsection d(5) equates the terms "Federal computer system", and "operator of a Federal computer system" to the meanings provided in section 18(c) of the NBS Act.

Section 5. Training by Operators of Federal Computer Systems

Subsection 5(a) requires each operator of a Federal computer system that contains sensitive information provide mandatory periodic training in computer security. Such training shall be conducted in accordance with appropriate guidelines and regulations and is to apply to all employees involved in the management, use or operation of computer systems.

Subsection 5(b) establishes that training shall start 60 days after the issuance of appropriate regulations. The goals of the training will be to enhance computer security awareness and encourage use of improved computer security practices.

Subsection 5(c) requires OPM to issue regulations within six months after enactment of the Act relating to the procedures and scope of the mandatory training to be provided and how it will be implemented.

Section 6. Additional Responsibilities for Computer Systems Security and Privacy

Subsection 6(a) requires each Federal agency within six months of the date of enactment of this Act to identify each Federal computer system, and system under development, that contains sensitive information and which is within or under the supervision of that agency.

Subsection 6(b) requires each Federal agency to develop a computer security plan within one year after enactment of this Act. Copies of the plan will be sent to NBS and NSA for comment. The Director of OMB is authorized to disapprove the plan. This plan will be included in the agency's five-year plan required under the Paperwork Reduction Act and will be revised annually.

Section 7. Definitions

Section 7 equates the terms "computer system", "Federal computer system", operator of a Federal computer system", and "Federal agency", to the same meanings as contained in section 18(c) of the NBS Act.

Section 8. Rules of Construction of Act

Section 8 provides that nothing in the Computer Security Act shall be construed (1) to constitute authority to withhold information sought under the Freedom of Information Act; or (2) to authorize any Federal agency to limit, restrict, regulate, or control the collection, maintenance, disclosure, use, transfer, or sale of any information (regardless of the medium in which the information may be maintained) that is—(A) privately-owned information; (B) Infor-

mation disclosable under the Freedom of Information Act or other law requiring or authorizing the public disclosure of information; or (C) information in the public domain.

COST ESTIMATE OF THE CONGRESSIONAL BUDGET OFFICE

The cost estimate prepared by the Congressional Budget Office under Sections 308(a) and 403 of the Congressional Budget Act of 1974 is contained in the following letter from its Director:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, May 4, 1987.

Hon. JACK BROOKS,
Chairman, Committee on Government Operations, House of Representatives, Rayburn House Office Building, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the attached cost estimate for H.R. 145, the Computer Security Act of 1987.

If you wish further details on this estimate, we will be pleased to provide them.

With best wishes,
Sincerely,

EDWARD M. GRAMLICH,
Acting Director.

1. Bill number: H.R. 145.
2. Bill title: Computer Security Act of 1987.
3. Bill status: As ordered reported by the House Committee on Government Operations, April 7, 1987.
4. Bill purpose: H.R. 145 would require the National Bureau of Standards (NBS) to establish a computer security standards program for those computer systems subject to the Brooks Act. The bill directs NBS to develop government-wide standards and guidelines, training programs, and validation standards to evaluate the effectiveness of computer security standards; and to work with the National Security Agency (NSA) and other agencies in developing these standards and guidelines and conducting research and studies. Based on recommendations submitted by the NBS, the Secretary of Commerce would be required to promulgate standards and guidelines for computer security. The bill would also establish a 13-member Computer System Security and Privacy Advisory Board composed of representatives of other federal agencies and the private sector.

Within six months after the date of enactment, H.R. 145 would require all federal agencies to identify each computer system that contains sensitive data. Each agency would be required to establish a plan for the security of each computer and related system previously identified within a year after the date of enactment, and to revise it annually as necessary. The bill would also require mandatory periodic training in computer security for all federal agency employees who manage, use or operate computer systems. Similar training would also be required for certain employees of private contractors and other organizations that process information on

behalf of the federal government, such as state and local governments.

5. Estimated cost to the Federal Government: CBO estimates that enactment of this bill would cost NBS about $4 million to $5 million annually beginning in fiscal year 1988. Additional costs for planning and training in computer security by all agencies throughout the federal government would probably cost $20 million to $25 million in 1988 and $15 million to $20 million in each fiscal year thereafter. To the extent that this legislation would reduce fraud or other financial losses, some savings could also result from enactment of this bill. It is not possible to quantify these potential savings at this time.

Basis of Estimate.—Under the National Security Decision Directive (NSDD) 145, which became effective in September 1984, the President gave the National Security Agency (NSA) responsibility for ensuring the security of all classified and certain other sensitive information transmitted by federal computers or telecommunications systems. If enacted, H.R. 145 would assign some of this authority to NBS, mainly in the area of unclassified data. Although under current guidelines it is expected that most federal agencies, with assistance from NSA, would have strengthened security efforts consistent with the directive, this bill would enhance the role of NBS and would also impose new requirements upon federal agencies and their contractors in the area of computer security.

National Bureau of Standards.—Assuming enactment of H.R. 145 and any necessary appropriations by October 1, 1987, the expanded role of NBS in compute security management and training is estimated to cost about $2 million annually beginning in 1988. Based on information from NBS, an estimated $2 million to $3 million annually may also be needed for research, beginning in 1988. This assumes that NBS would expand its management and oversight role, but would also receive assistance and information from the National Computer Security Center (NCSC) within the Department of Defense (DoD).

Government-wide computer security plans.—The level of computer security varies greatly among the approximately 80 federal entities, including about 1,300 different organizations that would be affected by this legislation. The cost of identifying all sensitive computer systems and developing an appropriate plan for facility, application and personnel security would thus vary greatly from agency to agency, depending upon the agency's current level of security, the size and number of sites, and the resources and expertise available to implement this provision.

CBO has not been able to contact each major federal entity to determine the cost of identifying and developing these plans for computer security. Based on the information available, it is expected that most agencies would probably assign existing personnel and resources to this task in order to meet the one-year deadline imposed by H.R. 145. If approximately 10,000 plans were developed, each requiring about 1-2 work weeks of effort by agency personnel, and two and one-half work days of review by NBS, NSA, and the Office of Management and Budget (OMB), the cost spread among the various federal agencies would be $10 million to $20 million over the fiscal years 1988 and 1989.

Government-wide training.—Currently, training resources in the area of computer security are scattered throughout the federal government. A few civilian agencies, such as the Department of Energy, have developed their own computer security training for both classified and unclassified systems. Most agencies, however, send employees to commercial courses or those offered by other federal agencies, such as the General Services Administration (GSA), the Office of Personnel Management (OPM), the Department of Agriculture Graduate School, or NSA.

H.R. 145 would require mandatory training for all federal and contractor personnel who manage, use or operate computer systems. The cost of such training depends on the number of people involved and the kind of training provided. Based on information from a number of agencies, it is expected that roughly half of all government and contractor employees, or about 3 million employees, would initially receive some type of training as a result of the bill. Subsequently, training would be provided to most new employees, and retraining would be required only periodically.

It is expected that most training in the area of computer security would become decentralized, with each agency responsible for developing its own programs, although some centralized training for smaller agencies and in specialized program areas would remain. The NCSC has developed a data base of educational opportunities offered by government, universities and private sources that is available to agencies. Training courses are relatively expensive, however. They currently cost about $50 to $200 per day per person (not including development costs) and typically are offered to technical personnel who attend a three-to-five day session. In an effort to reduce training costs, NCSC is developing training packages that will be available on tape or film, sharply reducing the training cost per person.

Based on information from NCSC, GSA, OPM, and OMB, CBO made a number of assumptions about the numbers and types of training that would be required as a result of enactment of H.R. 145. The resulting estimates provide a rough estimate of the possible additional cost of training, but should not be considered precise.

Within three years after the date of enactment, it is assumed that about 90 percent of the estimated 3 million employees affected by the bill would receive some type of computer security awareness training. Assuming the availability of training modules and other low-cost products, it is expected that the cost for this type of training would have no significant budget impact over and above the cost of maintaining good information systems, which is now the responsibility of each agency. It is estimated that about 10 percent of the 3 million employees, or 300,000, would require more formalized training. Assuming that about three quarters of these individuals (about one-half from DoD) would have received training under current law, then about 75,000 employees would likely require training as a result of this bill. Three days of specialized training, at an average cost of $100 per day, for 75,000 persons would cost $20 million to $25 million over several years. After the initial training, costs for retraining and training of new personnel are expected to cost about $5 million annually.

Finally, it is assumed that about 250 civilian employees would gradually be recruited and/or trained to evaluate the technical protection capabilities of industry nd government-developed systems, and to train other agency personnel. This type of training, according to NCSC, takes two to three years. At an average cost of $60,000 per year, including overhead, it is estimated that this tpe of support staff would cost the federal government about $15 million annually, once fully implemented.

6. Estimated cost to State and local governments: H.R. 145 would require nonfederal entities that process data on behalf of the federal government to provide security training. This requirement would also apply to nonfederal entities that maintain data for ultimate federal use, or that are involved in disbursing federal funds. No complete inventory of the relevant systems currently exists, and it is not possible at this time to estimate with precision the costs to state and local governments. Based on the limited information available, we expect that total costs incurred by state and local governments are likely to be less than $25 annually.

7. Estimate comparison: None.

8. Previous CBO estimate: None.

9. Estimate prepared by: Carol Cohen (226–2860).

10. Estimate approved by: C.G. Nuckols (for James L. Blum, Assistant Director for Budget Analysis).

Inflationary Impact

In compliance with clause 2(l)(4) of House Rule XI, it is the opinion of the Committee that the provisions of this bill will have no inflationary impact on prices and costs in the operation of the national economy.

Oversight Findings

The Committee has maintained continuous oversight of the government's acquisition and use of information technology. The Committee's findings are incorporated into this report.

New Budget Authority and Tax Expenditures

No new budget authority or tax expenditures are required by the legislation.

Budget Analysis and Projection

The bill provides for new authorization rather than new budget authority. Therefore, the provisions of Section 308(a) of the Congressional Budget Act are not applicable.

Changes in Existing Law Made by the Bill, as Reported

In compliance with clause 3 of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

ACT OF MARCH 3, 1901

* * * * * * *

SEC. 2. The Secretary of Commerce (hereinafter referred to as the "Secretary") is authorized to undertake the following functions:

(a) * * *

* * * * * * *

(f) Invention and development of devices to serve special needs of the Government.

In carrying out the functions enumerated in this section, the Secretary is authorized to undertake the following activities and similar ones for which need may arise in the operations of Government agencies, scientific institutions, and industrial enterprises:

(1) * * *

(18) the prosecution of such research in engineering, mathematics, and the physical sciences as may be necessary to obtain basic data pertinent to the functions specified herein; [and]

(19) the compilation and publication of general scientific and technical data resulting from the performance of the functions specified herein or from other sources when such data are of importance to scientific or manufacturing interests or to the general public, and are not available elsewhere, including demonstration of the results of the Bureau's work by exhibits or otherwise as may be deemed most effective, and including the use of National Bureau of Standards scientific or technial personnel for part-time or intermittent teaching and training activities at educational institutions of higher learning as part of and incidental to their official duties and without additional compensation other than that provided by law[.] ;

(20) the study of computer systems (as that term is defined in section 20(d) of this Act) and their use to control machinery and processes.

* * * * * * *

SEC. 20. (a) The National Bureau of Standards shall—

(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code;

(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code; and

(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive

order or an Act of Congress to be kept secret in the interest of national defense or foreign policy,

the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 111(d) of the Federal Property and Administrative Services Act of 1949;

(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987; and

(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

(b) In fulfilling subsection (a) of this section, the National Bureau of Standards is authorized—

(1) to assist the private sector, upon request, in using and applying the results of the programs and activities under this section;

(2) to make recommendations, as appropriate, to the Administrator of General Services on policies and regulations proposed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

(3) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

(4) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987;

(5) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost effective security and privacy of sensitive information in Federal computer systems; and

(6) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)—

(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a) (3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal com-

puter 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.

(c) For the purposes of (1) developing standards and quidelines under subsection (a)(3), and (2) performing research and conducting studies under subsection (b)(5), the National Bureau of Standards shall draw on the technical advice and assistance (including work products) of the National Security Agency, where appropriate.

(d) AS used in this section—

(1) the term "computer system"—

(A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

(B) includes—

(i) computers;

(ii) ancillary equipment;

(iii) software, firmware, and similar procedures;

(iv) services, including support services; and

(v) related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949;

(2) the term "Federal computer system"—

(A) means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function; and

(B) includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949;

(3) the term "operator of a Federal computer system" means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function;

(4) the term "sensitive information" means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

(5) the term "Federal agency" has the meaning given such term by section 3(b) of the Federal Property and Administrative Services Act of 1949.

SEC. 21. (a) There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the

Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industry;

(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

(b) The duties of the Board shall be—

(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining the Federal computer systems; and

(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate Committees of the Congress.

(c) The term of office of each member of the Board shall be four years, except that—

(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

(d) The Board shall not act in the absence of a quorum, which shall consist of seven members.

(e) Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

(f) To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency.

(g) As used in this section, the terms "computer system" and "Federal computer system" have the meanings given in section 20(d) of this Act.

SEC. [20.] *22.* Appropriations to carry out the provisions of this Act may remain available for obligation and expenditure for such period or periods as may be specified in the Acts making such appropriations.

SEC. 23. This Act may be cited as the National Bureau of Standards Act.

SECTION 111 OF THE FEDERAL PROPERTY AND ADMINISTRATIVE SERVICES ACT OF 1949

AUTOMATIC DATA PROCESSING EQUIPMENT

SEC. 111. (a) * * *

* * * * * * *

[(d) The Secretary of Commerce is authorized (1) to provide agencies, and the Administrator of General Services in the exercise of the authority delegated in this section, with scientific and technological advisory services relating to automatic data processing and related systems, and (2) to make appropriate recommendations to the President relating to the establishment of uniform Federal automatic data processing standards. The Secretary of Commerce is authorized to undertake the necessary research in the sciences and technologies of automatic data processing computer and related systems, as may be required under provisions of this subsection.]

"(d)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 20(a) (2) and (3) of the National Bureau of Standards Act, promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems. The President may disapprove or modify such standards and guidelines if he determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be submitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

(2) The head of a Federal agency may employ standards for the cost effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

(3) The standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or cause a major adverse financial impact on the operator which is not offset by government-wide savings. The Secretary may delegate to the head of one or more Federal agencies authority to waive such standards to the extent to which the Secretary determines such action to be

necessary and desirable to allow for timely and effective implementation of Federal computer systems standards. The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of title 44, United States Code. Notice of each such waiver and delegation shall be transmitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register.

(4) The Administrator shall revise the Federal information resources management regulations (41 CFR ch. 201) to be consistent with the standards and guidelines promulgated by the Secretary of Commerce under this subsection.

(5) As used in this subsection, the terms "Federal computer system" and "operator of a Federal computer system" have the meanings given in section 20(d) of the National Bureau of Standards Act.

* * * * * * *

○

Document No. 4