Appendix B: Computer Security Act and Related Documents

B

Public Law 100-235
100th Congress

An Act

Jan 8, 1988
[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.

Be *it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

Computer Security Act of 1987.
Classified information.
40 USC 759 note.

SECTION 1. SHORT TITLE.

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

40 USC 759 note.

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 assistance (including work products) of the National Security Agency, where appropriate;

(2) to provide for promulgation of such standards and guidelines by amending section ill(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. 271-278 h), is amended—

15 USC 272.

(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.";

15 USC 278h

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

15 USC 27&z-3

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

"(l) 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 (l), (2), and (3) of this subsection through research and liaison with other government and private agencies.

"(%) 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 ill(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 Manage- Regulations.
ment 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 for the protection of sensitive information in Federal computer systems under subsections (a)(l) and (a)(3), and

"(2) performing research and conducting studies under subsection (b)(5),

the National Bureau of Standards shall draw upon 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.

"(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 o rated 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 ill(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 Is USC 278g-4
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:

"(l) 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 industries;

"(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-

"(l) 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 Reports.
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 ear, 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 sub chapter 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:

National Bureau of Standards Act. 15 USC 271 note.

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

SEC. 4. AMENDMENT TO BROOKS ACT.

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

"(d)(l) 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.

President of U.S.

Federal Register, publication.

"(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 time] 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

Federal Register, publication,

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. Regulations

"(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. FEDERAL COMPUTER SYSTEM SECURITY TRAINING. 40 USC 759 not-e,

(a) IN GENERAL.—Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency. Such training shall be—

(1) provided in accordance with 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 Federal civilian employees; or

(2) provided by an alternative training program approved by the head of that agency on the basis of a determination that the alternative training program is at least as effective in accomplishing the objectives of such guidelines and regulations.

(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 systems; 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 Federal civilian employees 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. 40 USC 759 note.

(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 risk and magnitude of the harm resulting *from* the loss, misuse, or unauthorized access 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.

40 USC 759 note

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).

40 USC 759 note

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

Public information.

(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.

Approved January 8, 1988.

LEGISLATIVE HISTORY--H.R. 145:

HOUSE REPORTS: No. 100-153, Pt. 1 (Comm. on Science, Space, and Technology) and Pt. 2 (Comm. on Government Operations).

CONGRESSIONAL RECORD, vol. 133 (1987):

June 22, considered and passed House.

Dec. 21, considered and passed Senate.

WEEKLY COMPILATION OF PRESIDENTIAL DOCUMENTS, Vol. 24 (1988):

Jan. 8, Presidential statement.

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE DIRECTOR OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
AND
THE DIRECTOR OF THE NATIONAL SECURITY AGENCY
CONCERNING
THE IMPLEMENTATION OF PUBLIC LAW 100-235

Recognizing that:

Under Section 2 of the Computer Security Act of 1987 (Public Law 100-235), (the Act), the National Institute of Standards and Technology (NIST) has the responsibility within the Federal Government for:

1. Developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems as defined in the Act; and,

2. Drawing on the computer system technical security guidelines of the National Security Agency (NSA) in this regard where appropriate.

B. Under Section 3 of the Act, the NIST is to coordinate closely with other agencies and offices, including the NSA, to assure:

1. 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,

2. To the maximum extent feasible, that standards developed by the NIST under the Act are consistent and compatible with standards and procedures developed for the protection of classified information in Federal computer systems.

C. Under the Act, the Secretary of Commerce has the responsibility, which he has delegated to the Director of NIST, for appointing the members of the Computer System Security and Privacy Advisory Board, at least one of whom shall be from the NSA.

Therefore, in furtherance of the purposes of this MOU, the Director of the NIST and the Director of the NSA hereby agree as follows:

I. The NIST will :

1. Appoint to the Computer Security and Privacy Advisory Board at least one representative nominated by the Director of the NSA.

2. Draw upon computer system technical security guidelines developed by the NSA to the extent that the NIST determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

3. Recognize the NSA-certified rating of evaluated trusted systems under the Trusted Computer Security Evaluation Criteria Program without requiring additional evaluation.

4. Develop telecommunications security standards for protecting sensitive unclassified computer data, drawing upon the expertise and products of the National Security Agency, to the greatest extent possible, in meeting these responsibilities in a timely and cost effective manner.

5. Avoid duplication where possible in entering into mutually agreeable arrangements with the NSA for the NSA support.

6. Request the NSA's assistance on all matters related to cryptographic algorithms and cryptographic techniques including but not limited to research, development, evaluation, or endorsement.

II. The NSA will:

1. Provide the NIST with technical guidelines in trusted technology, telecommunications security, and personal identification that may be used in cost-effective systems for protecting sensitive computer data.

2. Conduct or initiate research and development programs in trusted technology, telecommunications security, cryptographic techniques and personal identification methods.

3. Be responsive to the NIST's requests for assistance in respect to all matters related to cryptographic algorithms and cryptographic techniques including but not limited to research, development, evaluation, or endorsement.

4. Establish the standards and endorse products for application to secure systems covered in 10 USC Section 2315 (the Warner Amendment) .

5. Upon request by Federal agencies, their contractors and other government-sponsored entities, conduct assessments of the hostile intelligence threat to federal information systems, and provide technical assistance and recommend endorsed products for application to secure systems against that threat.

III. The NIST and the NSA shall:

1. Jointly review agency plans for the security and privacy of computer systems submitted to NIST and NSA pursuant to section 6(b) of the Act.

2. Exchange technical standards and guidelines as necessary to achieve the purposes of the Act.

3. Work together to achieve the purposes of this memorandum with the greatest efficiency possible, avoiding unnecessary duplication of effort.

4. Maintain an ongoing, open dialogue to ensure that each organization remains abreast of emerging technologies and issues effecting automated information system security in computer-based systems.

5. Establish a Technical Working Group to review and analyze issues of mutual interest pertinent to protection of systems that process sensitive or other unclassified information. The Group shall be composed of six federal employees, three each selected by NIST and NSA and to be augmented as necessary by representatives of other agencies. Issues may be referred to the group by either the NSA Deputy Director for Information Security or the NIST Deputy Director or may be generated and addressed by the group, upon approval by the NSA DDI or NIST Deputy Director. Within 14 days of the referral of an issue to the Group by either the NSA Deputy Director for Information Security or the NIST Deputy Director, the Group will respond with a progress report and plan for further analysis, if any.

6. Exchange work plans on an annual basis on all research and development projects pertinent to protection of systems that process sensitive or other unclassified information, including trusted technology, technology for protecting the integrity and availability of data, telecommunications security and personal identification methods. Project updates will be exchanged quarterly, and project reviews will be provided by either party upon request of the other party.

7. Ensure the Technical Working Group reviews prior to public disclosure all matters regarding technical systems security techniques to be developed for use in protecting sensitive information in federal computer systems to ensure they are

consistent With the national security of the United States. If NIST and NSA are unable to resolve such an issue within 60 days, either agency may elect to raise the issue to the Secretary of Defense and the Secretary of Commerce. It is recognized that such an issue may be referred to the President through the NSC for resolution. No action shall be taken on such an issue until it is resolved.

8. Specify additional operational agreements in annexes to this MOU as they are agreed to by NSA and NIST.

Iv. Either party may elect to terminate this MOU upon six months written notice.

This MOU is effective upon approval of both signatories.

Raymond G. Kammer

RAYMOND G. KAMMER
Acting Director
National Institute of
Standards and Technology

DATE: Mar 24, 1989

W. O. Studeman

W. O. STUDEMAN
Vice Admiral, U.S. Navy
Director
National Security Agency

DATE: 23 March 1989

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
(formerly National Bureau of Standards)
Gaithersburg, Maryland 20899
OFFICE OF THE DIRECTOR

22 December 1989

Honorable John Conyers, Jr.
Honorable Frank Horton
Committee on Government Operations
2157 Rayburn House Office Building
House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman and *Mr.* Horton:

This is to answer certain questions raised at the hearing on May 4, 1989 before your Committee regarding the Memorandum of Understanding (MOU) between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). As Chairman Conyers suggested during the hearing, representatives of our two agencies have met with Mr. Milton Socolar and others of the General Accounting Office (GAO) to better understand your Committee's and GAO's concerns about the MOU and to clarify the intent and proper interpretation of that document. Further, we provided Mr. Socolar with a draft of this letter to ensure that we have accurately identified the major points of concern raised by GAO and your Committee.

Following another of the Committee's suggestions, we also contacted witnesses who testified at the hearing to discuss their concerns and explain the intent and proper interpretation of the MOU. We have attempted also to respond as fully as possible in this letter to the concerns raised by those parties.

One central concern of the witnesses at the hearing, including GAO, was that the MOU may have sought to weaken the essential purpose of the Computer Security Act of 1987 (the Act) -- i.e., to commit entirely to NIST, a civilian agency with the requisite expertise, the full responsibility for security standards for government computer systems containing unclassified but sensitive information. At the outset, let us emphatically assure you that our agencies had no such intent. To the contrary, we regard the MOU as a document implementing the Act by outlining areas of necessary agency interaction in support of the NIST Computer Security Program -- which Program involves many other activities of NIST. But it is easy in retrospect to see that a document focused solely on points of NSA/NIST interaction might cause a false impression of the relative importance within the Program of the two agencies' activities and roles. NIST's unquestioned Program direction, as well as the great bulk of activities which are NIST's exclusive domain -- like 9/10ths of an iceberg -- remained undisplayed in the MOU.

Both NIST and NSA are keenly aware of the significant changes in the administration of NIST's program that *were* mandated by the Computer Security Act, and fully support the Act and its intent. The Act has strengthened the authority of the Secretary of Commerce in the preparation and promulgation of Federal Information Processing Standards (FIPS) and guidelines for the protection of unclassified information stored in federal computer systems. Before the Act was passed, the basic authority for promulgating FIPS rested with the President under the Brooks Act, with the role of the Secretary of Commerce being delegated through Executive Order 11717. Delegated authority is inherently susceptible of weakening or re-definition by the delegating official.

The Act not only placed the government computer security program for systems that process sensitive unclassified information explicitly and directly into the hands of the Secretary of Commerce, but suppressed any erosion of the Secretary's authority that might have been threatened by the 1985 promulgation of National Security Decision Directive (NSDD) - 145, "National Policy on Telecommunications and Automated Information Systems Security." NSDD-145 obliged Commerce to submit to an interagency review of FIPS just before they were to be issued by the Secretary -- a step viewed by many as undermining Commerce authority to issue FIPS and as an intrusion of military-related agencies, particularly NSA, into civilian matters. Finally, NSDD-145, and more particularly certain policy documents issued pursuant to it, had been interpreted by some to give the Department of Defense and NSA authority to make determinations regarding what information in computers required protection. Since passage of the Act, it has been recognized that such policies have no applicability to systems within the purview of the Act. This recognition is reflected in the letter to Chairman Conyers from the Assistant to the President for National Security Affairs, dated June 26, 1989.

Just as important as the direct authority the Act lodged with the Secretary of Commerce was the Act's careful, narrow definition of that authority, which implies strict limits on the scope of the NIST Computer Security Program. The power of the Secretary is limited to promulgating standards and guidelines for hardware and software to protect the unclassified but sensitive information contained in federal computer systems. The Act confers no power to issue any standard regulating the types of information such systems may contain or who may be given access to such information. These matters are entirely the responsibility of individual agencies.

In drafting the MOU, both agencies considered the intent of the Computer Security Act to be both paramount and plain. We accepted as a given that NIST, not NSA, has the responsibility and authority to set security standards applicable to Federal Government computer systems that contain sensitive but unclassified

information. Similarly clear in our minds was that NSA's role vis-a-vis the security of these systems is solely to provide the benefits of relevant NSA technical expertise for NIST to use as it sees fit. Having no confusion regarding the two agencies' basic roles under the Act, we saw no need to recite them in the MOU. Nor, as we mentioned above, did we see a need to detail the many specific activities or programs NIST may undertake in implementing the Act. Our purpose was simply to express positively (1) the interrelationship between NIST and NSA to implement the purposes of the Act, and (2) our understandings regarding NSA programs or activities which overlap with or are affected by NIST activities under the Act.

The concerns of GAO focused on four areas in the MOU. In particular, GAO viewed the 'scope of activities for the Technical Working Group it establishes to be unclear and to raise uncertainties about the *extent* of NSA involvement in NIST functions. In three other areas, GAO considered the MOU "not clear about the respective roles of NSA and NIST." All four areas of concern are outlined below, and clarification is provided. The areas primarily involving no more than an apparent imbalance in the statement of agency roles are discussed first.

a. The inclusion of research and development activities for NSA but not for NIST.

Clarification: As we explained earlier, the MOU was intended to outline only areas of helpful agency interaction in support of the NIST Computer Security Program. We did not undertake to recite NIST's program direction *or its* many independent computer security-related activities. Such a recitation would have been particularly unnecessary in the R&D area because the Act clearly gives NIST the authority and duty to conduct research and development. Indeed, NIST does significant computer security R&D and expects to continue this work. The provision of the MOU relating to R&D was intended: (i) to acknowledge by implication that NSA's R&D aimed at securing systems handling classified information may apply to the systems whose protection is NIST's responsibility; and (ii) to acknowledge that NSA will continue these R&D efforts and affirm that NSA will make their results available to NIST as appropriate.

b. The automatic acceptance *of* NSA evaluations *of* Trusted Systems as sufficient for NIST program purposes.

Clarification: This provision reflects the understanding and intent of Congress in passing the Act that NIST (then NBS) would not require computer system developers to put their systems through a certification process by NIST after they had passed the stringent requirements NSA imposes upon systems handling **classified** materials. Section 4 of the Act mandates the essence of this policy by amending section Ill(f) of the Federal Property

and Administrative Services Act to include a subsection (2) reading:

> (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.

As Senator Roth explained:

> ... The process of testing and validating [computer security] systems for use by the Federal Government, particularly our defense and intelligence agencies, is very rigorous and can take a long time. Some [private firms which are in the business of developing such systems] . . . were concerned that they might be forced to run the gauntlet twice: once through NSA's National Computer Security Center and then again through the National Bureau of Standards. I have been assured by NBS that, once a system has passed muster at NSA'S Computer Security Center, it would not have to go through the NBS process for use by agencies with unclassified systems. If the system provides the additional safeguarding required for classified systems, it would clearly be sufficient for use by agencies with unclassified systems. (Cong. Rec. S18637, Dec. 21, 1987.)

The Committee may wonder why our two agencies decided to recite in the MOU a policy that primarily benefits third parties -- i.e., federal "user" agencies and developers of NSA-certified systems. The purpose was to assure NSA that NIST will accept NSA trusted system evaluations and burden neither agency with consultations on superfluous additional protections. Finally, we note that although this provision of the MOU indicates that NIST will 'recognize the NSA-certified ratings . . . without requiring additional evaluation," it is not meant to suggest an identity between NIST's criteria and those of NSA. Nor does it require that NSA trusted systems criteria be met by systems subject to NIST standards.

c. Mention in the MOU of NSA's threat assessments of information systems without corresponding mention of the NIST role in assessing information system vulnerability.

Clarification: GAO indicated a concern that by mentioning only the NSA role in conducting assessments of the hostile intelligence threat to federal information systems, the MOU "suggests a diminution of NIST responsibilities for assessing computer system vulnerability. As we will explain, your Committee can be assured that it was not our intent in this or any other part of the MOU to diminish NIST's leadership or operating responsibilities under the Act.

Once again we note that the MOU was intended to outline only areas of agency interaction -- not to recite NIST's independent computer security-related activities. As with R&D, this provision of the MOU relates to an area in which both agencies have ongoing activities. The NIST responsibility to assess computer system vulnerabilities is clear in the Act and its legislative history. As then-Chairman Brooks said, the Act "sets up an important research program within [NIST] to assess the vulnerability of government computers and programs." (Cong. Rec. H6017, Aug. 12, 1986.) NIST is pursuing these activities diligently and will continue to do so.

NSA has a program that draws upon its unique expertise in assessing hostile intelligence threats. As an adjunct of this program, NSA evaluates the vulnerability of computer systems to such threats. NSA conducts its hostile intelligence threat and vulnerability assessments upon request of the individual agencies that operate computer systems. By noting in the MOU that NSA will continue to conduct such assessments upon the request of 'federal agencies, their contractors and other government-sponsored entities, "we simply meant to make clear to all concerned that in cases involving NSA's unique expertise, NIST will not, and should not be expected to, duplicate NSA's special role of evaluating hostile intelligence threats. The phrase 'hostile intelligence threats" is understood by both agencies as a reference to the threat of foreign exploitation.

d. The scope of activities of the Technical Working Group.

This concern of GAO, shared by Committee staff, is more complex. As Mr. Socolar explained it in his testimony:

> Section 111.5 of the MOU establishes a Technical Working Group to review and analyze issues of mutual interest pertinent to protection of systems that process sensitive, unclassified information. The group

> will consist of six federal employees, three each selected by NIST and NSA. Under section 111.7, the group will review, prior to public disclosure, all matters regarding technical security systems techniques to be developed for use in protecting sensitive information to ensure they are consistent with the national security. If NIST and NSA are unable to resolve an issue within 60 days, either agency may raise the issue to the Secretary of Defense and the Secretary of Commerce. Such an issue may be referred to the President through the National Security Council (NSC) for resolution. The MOU specifies that no action is to be taken on such an issue until it is resolved. These provisions appear to give NSA more than the consultative role contemplated under the Act. They seem to give NSA an appeal process -- through the National Security Council -- leading directly to the President should it disagree with a proposed NIST standard or guideline. The Act provides that the President may disapprove any such guidelines or standards promulgated by the Secretary of Commerce, that this disapproval authority cannot be delegated, and that notice of any such disapproval or modification must be submitted to the House Committee on Government Operations and the Senate Committee on Governmental Affairs. Under section 111.7 of the MOU, it appears that an avenue has been opened which would invite presidential disapproval or modification of standards and guidelines in advance of promulgation by the Secretary without proper notification to the Congress.

Here Mr. Socolar correctly noted that in NIST'S view (which is shared by NSA) the provision defining the Working Group's function as being to “review matters . . . <u>to be developed</u>” limits the scope of the ‘appeal process" to proposed research and development projects in new areas. However, he responded to this point by saying:

> If this provision pertains only to research and development, it still gives NSA a significant role in what were to be NIST functions under the Act. NSA could cause significant delay of a project NIST deems warranted, and it would appear that in matters of disagreement, Commerce has placed itself in a position of having to appeal to the President regardless of its own position.

<u>Clarification</u>: The Technical Working Group provides the essential structure within which NIST and NSA can conduct the techni-

cal discussions and exchange contemplated by the Act. As we explain below:

> (i) its balanced membership reflects the balanced, two-way nature of technical consultations required by the Act: and
>
> (ii) the "appeal mechanism" in the MOU is consistent with normal NIST procedures which the Act contemplates will be used in implementing the Computer Security Program, and in any case is a prudent exercise of Commerce Department discretion to carry out the purposes of the Act.

With this explanation, we hope the Committee will understand that neither the Working Group provisions of the MOU nor its "appeals procedure" are intended to dilute NIST control over its Computer Security Program or are likely to have that effect.

The Working Group is established within the framework of Section III of the MOU, which addresses a number of technical areas of mutual NIST and NSA interest and responsibility under the Act. Such areas within the Act include, for example, section 6 which requires operators of federal computer systems containing sensitive but unclassified information to forward their system security plans "for advice and comment" not only to NIST, but directly to NSA as well. Even more importantly, the Act contemplates two-way interagency communication of technical computer security information and ideas -- not just from NSA to NIST or vice versa, and not just about NIST'S program.

While the Act puts NIST in full charge of the Computer Security Program, it wisely avoids requiring interagency technical consultations on computer security matters to be exclusively one-way communications. In addition to NSA's consultative role to NIST, the Act not only contemplates, but requires, that each agency consult with the other in developing its programs. As former OMB Director James Miller assured Congress: "When developing technical security guidelines, NSA will consult with [NIST] to determine how its efforts can best support [NIST's program] requirements." (Cong. Rec. S18636, Dec. 21, 1987.)

If the Act had adopted a one-way approach, we would likely soon find ourselves with unrelated and possibly incompatible sets of computer security standards, or at least with considerable overlapping and duplication of effort in this area. As Senator Leahy explained at the time of Senate consideration of the bill:

> This legislation does not mandate or even urge the establishment of two sets of data security standards or systems. Instead, it provides a framework for recognizing and reconciling the sometimes differing security needs of these distinct communities. (Id.)

Apart from the need to establish a process for consultation on technical systems security matters, the parties recognized that the public development or promulgation of technical security standards of specific types, particularly regarding cryptography, could present a serious possibility of harm to the national security. Such problems need to be identified and resolved before the public becomes involved in the standards development process.

Issues in this narrow class are the only matters to which the 'appeals process" of section 111.7 applies. These problems are outside the category of "sensitive but unclassified" matters, sole concern to NIST and well within the national security framework of concern to NSA, other Executive Branch agencies and the President. GAO, your Committee staff and others with whom we have spoken in connection with the MOU readily acknowledge the potential national security impact of premature or inappropriate agency action in the computer security area.

The NIST procedures allow complete public involvement at a very early stage in the standards research and development process -- usually years before a standard is promulgated as a result of a particular effort. By and large, when NIST and NSA first discuss a possible new standard or technique from a technical standpoint, its actual promulgation is a very distant potential. Indeed, it is at this stage that Commerce normally consults with OMB, and potentially with the President, about funding for significant research efforts. The appeals procedure is hardly distinguishable from those consultations -- since either procedure can result in dropping or modifying a proposed course of action. Although we fully understand GAO's and your Committee's concern and careful oversight of this matter in light of the purposes of the Act, the appeals procedure will not in practice "invite Presidential disapproval or modification of standards and guidelines . . . without proper notification to the Congress."

Nor has Commerce, by agreeing to such a procedure, bound itself to anything "regardless of its position." Under no circumstances would Commerce consider taking an action in the computer security area which, due to an unresolved issue involving technical methods, might harm the national security. Thus, only to the most trivial and theoretical degree can it be said that Commerce, by agreeing to resolve such issues before acting in this area, has diluted its responsibility for the promulgation of standards and guidelines.

We wish to emphasize to the Committee that the 'national security" nexus that must be present under paragraph 111.7 completely precludes appeals of issues of any other type. Finally, the mention of the National Security Council in paragraph 111.7 of the MOU does not imply any role for the NSC staff in considering

such issues and, most emphatically, not in the computer security standard setting process. This reference to the NSC was made only to suggest that it is likely that this statutory body consisting of the President, Vice President, Secretary of State, and Secretary of Defense would be the appropriate body to advise the president on the national security matters that may arise in this context. Moreover, for consideration of such issues, the National Security Council would undoubtedly be augmented by the Secretary of Commerce.

With this background, it should be clear that the MOU does not, as some have suggested, give NSA a "veto" over NIST activities or over its promulgation of standards and guidelines. The appeals procedure simply ensures that certain issues can be resolved in a timely fashion so that the Program can proceed smoothly.

Our conversations with private sector witnesses have revealed that many of their concerns coincided with or were similar to those identified by the GAO, and thus are addressed above. One additional area of concern they raised, which was echoed by some of the staff of your Committee, was that the MOU might in some way undercut existing legal controls on NSA's abilities to conduct electronic surveillance, or otherwise empower NSA to use the NIST Computer Security Program for purposes outside the scope of that Program. We can assure everyone concerned that such misuse is simply not possible -- because NIST, which has no intelligence or military functions, is in charge of this Program, and the Program does nothing more than develop standards for protecting certain information systems. Moreover, the Program has been, and will continue to be, implemented in full compliance with all applicable laws, including the Privacy Act and the Freedom of Information Act.

To ensure that our successors and others can read the MOU in light of our intent and the clarification we provide in this letter, we are appending this letter to the MOU. We hope this has fully answered the questions raised by your Committee and the others who have indicated similar concerns. We are confident that the NIST/NSA implementation of the MOU over the coming months and years will lay to rest concerns that NIST and NSA may not adhere to their respective roles under the Act.

NIST

W.O. Studeman

NSA

THE SECRETARY OF COMMERCE
Washington, D.C. 20230

FEB 23 1990

Honorable John Conyers
Chairman, Committee on
Government Operations
House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

This letter responds to your inquiry about the Memorandum of Understanding (MOU) between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) relating to the Computer Security Act.

We have worked diligently to address the concerns that you have expressed about the MOU. In a letter to you from NIST and NSA dated December 22, 1989, we responded to each specific concern and explained why we believe the MOU is consistent with the principles of the Computer Security Act. We have also fully considered additional points that were raised orally by the Committee staff after our submission of the joint NIST/NSA letter to the Committee. For reasons explained in the enclosed paper, the concerns expressed by the staff have not changed our opinion that the MOU, particularly when read in conjunction with our subsequent letter, properly carries out both the letter of the law and the intent of the Congress.

I hope that the enclosed paper will allay your remaining concerns about specific provisions of the MOU. But in any event, because of the importance of this issue, I have asked Deputy Secretary Thomas Murrin to act on my behalf in this matter and to meet with you and Congressman Horton to discuss the issues regarding this Department's commitment to the principles of the Computer Security Act.

Your letter also requests copies of all documents relating to topics addressed by the Technical Working Group established by the MOU. I suggest that we await the outcome of your meeting with Deputy Secretary Murrin before we address our response to your request.

I have asked my Assistant Secretary for Legislative and Intergovernmental Affairs, William Fritts, to get in touch with your office shortly to set up a time for this meeting.

Sincerely,

Robert A. Mosbacher

Enclosure

cc: Honorable Frank Horton

COMPUTER SECURITY -- NIST/NSA MEMORANDUM OF UNDERSTANDING

Matters Raised by House Government Operations Committee Staff

at Meetinq on Januany 3, 1990

On January 3, 1990, Commerce staff met with staff of the Government Operations Committee, at their request, to discuss the joint letter signed December 22, 1989, by NIST and NSA. The Committee staff expressed dissatisfaction with the joint NIST/NSA letter and said they believed there were still substantive problems in the MOU. The Committee staff's concerns were:

- that the MOU sets up a Technical Working Group which they believe serves only to delay NIST's computer security work, and which inappropriately has taken up matters that are not limited to national security issues.
- that the MOU inappropriately "invites" NSA to initiate R&D applicable solely to the NIST program.
- that the MOU should provide for NIST's oversight of the "cost effectiveness" of agency decisions to Use Systems NSA has certified for handling classified materials before accepting these highly-protected systems as automatically meeting NIST standards.
- that the MOU should provide that NSA cannot respond to agency requests to assess hostile intelligence threats to computer systems without going "through" NIST.

This paper addresses each in turn.

TECHNICAL WORKING GROUP

The Committee staff indicated that they believe the Technical Working Group (TWG) set up by the MOU serves only to delay NIST in developing standards and noted that the TWG has not entertained only matters which (in the words of the joint NIST/NSA letter) "could present a serious possibility of harm to the national security."

Comment. Rather than being a source of delay, the TWG is a critical aid to the NIST program. As explained in the

December 22 letter, the TWG 'provides the essential structure within which NIST and NSA can conduct the technical discussions and exchange contemplated by the [Computer Security] Act." We cited legislative history of the Act showing that Congress recognized the need for technical consultations between NIST and NSA to reconcile the differing security needs of the distinct communities these agencies serve, while avoiding duplication of effort or the development of unrelated and possibly incompatible sets of standards. For these reasons we believe it clear that the TWG -- or something like it -- was not only contemplated by the Computer Security Act, but is indispensable to fulfilling the Act's mandate.

Also, the TWG does not consider only matters having special national security implications. The December 22 letter explained that the TWG considers all technical computer security matters of mutual interest to NIST and NSA, while the national security restriction serves only to limit the scope of matters subject to the 'appeals process." The TWG has considered several issues, but the appeals process has not been used to date.

WHETHER THE MOU INVITES NSA R&D WITH APPLICABILITY SOLELY TO NIST's PROGRAM

The staff re-affirmed its belief that the provision of the MOU relating to NSA computer security research invites NSA to self-initiate R&D solely to provide security measures for computer systems under NIST's jurisdiction.

Comment. As we noted in the joint NIST\NSA letter, this provision was intended simply to acknowledge that NSA research may have applicability to systems whose protection is NIST's responsibility -- and to affirm that NSA will continue its research efforts and make their results available to NIST as appropriate. Since the provision does not speak to the issue of NSA self-initiation of R&D solely for NIST program use, and since both agencies have disclaimed such a meaning in an official letter of clarification of the MOU, we see no remaining basis for this interpretation.

Furthermore, research with applicability solely to computers handling sensitive but unclassified materials would be rare. Most computer security research deals with technical problems, hardware, or methods whose applicability to a particular system would not depend on the type of information the system contains. Thus, almost all research NSA might undertake would have at least potential applicability to both agencies' programs.

ACCEPTANCE OF NSA-CERTIFIED SYSTEMS
AS MEETING NIST STANDARDS

The staff argued that instead of automatically accepting NSA-certified systems as meeting our standards, NIST has a duty to determine (or set criteria for determining) whether the NSA-certified system is "cost-effective" for the agency involved. The words "cost effective" in section 4 of the Computer Security Act were cited as supporting the existence of this duty.

Section 4 amended section 111(d) of the Federal Property and Administrative Services Act to include a section reading:

> (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 . . . 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. (Emphasis added; currently codified at 40 U.S.C. ill(d).)

Comment. At the hearing last May, the GAO witness questioned the general policy stated in the MOU concerning NIST's automatic acceptance of NSA-certified systems. Our letter responded by showing that this was a positive legal requirement. The Committee staff did not challenge that demonstration, but implied that the cost effectiveness of an agency's decision to use the more stringent NSA safeguard is an exception to this requirement and something NIST should oversee.

First, we note that this issue really does not involve the MOU, which deals only with matters between NIST and NSA. If NIST were to set cost-effectiveness criteria, it would do so through rulemaking rather than by amending the MOU.

Second, Congress clearly withheld from NIST the authority to determine for other agencies the "cost effectiveness" of their decisions to use NSA-certified systems. The relevant portion of section 4 of the Computer *Security* Act confers power on the heads of agencies generally, and is not directed toward NIST. The Act does allow NIST to waive its standards to avoid major adverse financial impact on agencies. However, the Act wisely avoids conferring upon NIST any general authority, much less a duty, to police other agencies' spending decisions. NIST, as a science-oriented agency, is not well suited for such a role. Also, the Act could not require centralized policymaking that has implications about which agencies may use which types of computer systems without undermining its overall intent to keep such

potentially sensitive decisions in the hands of individual agencies.

NIST is concerned with cost-effectiveness, but its responsibility for this element is centered on its own standards and guidelines. This is reflected in the wording of section 2 of the Act which charges NIST with setting "standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems."

NSA ASSESSMENTS OF HOSTILE INTELLIGENCE THREATS

The MOU recites that upon the request of agencies or their contractors, NSA will evaluate the susceptibility of computer systems to hostile intelligence threats. The staff did not question that this is an NSA function. However; 'they argued that NSA should not do this upon direct agency request, but only through NIST, because a theme of the Act was to divorce NSA from direct involvement with computer systems handling solely non-classified materials.

Comment. To evaluate this suggestion, it is important to note the fundamentally different nature of (a) assessments of the vulnerability of computer systems as such, and (b) assessments of hostile intelligence threats to such systems. The MOU provision on this issue emphasizes that hostile intelligence threat assessment is uniquely an NSA capability which NIST cannot and should not be expected to duplicate.

The Committee staff suggestion would inject a NIST referral into the process of agency requests for hostile intelligence threat assessments by NSA. There would be no point in creating such a step unless NIST had some basis for evaluating the need for this NSA service. NIST has no expertise in this area and thus no basis for judging whether an agency reasonably needs an assessment of possible hostile intelligence threats to its system.