Calendar No. 718

105th Congress 2d Session	SENATE	REPORT 105–412

COMPUTER SECURITY ENHANCEMENT ACT OF 1997

REPORT

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ON

H.R. 1903

OCTOBER 13 (legislative day, OCTOBER 2), 1998.—Ordered to be printed

---

U.S. GOVERNMENT PRINTING OFFICE
69–010 WASHINGTON : 1998

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

JOHN McCAIN, Arizona, *Chairman*

TED STEVENS, Alaska
CONRAD BURNS, Montana
SLADE GORTON, Washington
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA SNOWE, Maine
JOHN ASHCROFT, Missouri
BILL FRIST, Tennessee
SPENCER ABRAHAM, Michigan
SAM BROWNBACK, Kansas

ERNEST F. HOLLINGS, South Carolina
DANIEL K. INOUYE, Hawaii
WENDELL H. FORD, Kentucky
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
JOHN B. BREAUX, Louisiana
RICHARD H. BRYAN, Nevada
BYRON L. DORGAN, North Dakota
RON WYDEN, Oregon

JOHN RAIDT, *Staff Director*
MARK BUSE, *Policy Director*
MARTHA P. ALLBRIGHT, *General Counsel*
IVAN A. SCHLAGER, *Democratic Chief Counsel and Staff Director*
JAMES S. W. DREWRY, *Democratic General Counsel*

105TH CONGRESS
2d Session

SENATE

REPORT
105–412

COMPUTER SECURITY ENHANCEMENT ACT OF 1997

OCTOBER 13 (legislative day, OCTOBER 2), 1998.—Ordered to be printed

Mr. MCCAIN, from the Committee on Commerce, Science, and Transportation, submitted the following

REPORT

[To accompany H.R. 1903]

The Committee on Commerce, Science, and Transportation, to which was referred H.R. 1903, "A Bill to amend the National Institute of Standards and Technology Act to enhance the ability of the National Institute of Standards and Technology to improve computer security, and for other purposes", having considered the same, reports favorably thereon without amendment and recommends that the bill do pass.

PURPOSE OF THE BILL

H.R. 1903, as reported, would reinforce the National Institute of Standards and Technology's (NIST) role of ensuring the security of unclassified information in Federal computer systems; promote technology solutions based on private sector offerings to protect the security of Federal computer systems; and provide for the assessment of the capabilities of information security products incorporating cryptography that are generally available outside the United States.

BACKGROUND AND NEEDS

The Computer Security Act of 1987 (P.L. 100–235) was passed by Congress following several years of hearings and debate. Motivation for the Act was sparked by the escalating use of computer systems by the Federal government and the requirement to ensure the security and privacy of unclassified, sensitive information in those systems. A broad range of Federal agencies had assumed responsibility for various facets of computer security and privacy, prompting concerns that Federal computer security policy lacked focus, unity, and consistency, and contributed to a duplication of effort.

In 1985, the Office of Management and Budget (OMB) issued Circular A–130, Management of Federal Information Resources, su-

perseding Circular A–71. Appendix III of Circular A–130, Security of Federal Automated Information Systems, defined a minimum set of controls for the security of Federal automated information systems.

Following enactment of the Computer Security Act of 1987, OMB updated Appendix III of OMB Circular A–130 to assist agencies in implementing the Act (OMB Bulletin 88–16). The Appendix was updated again in 1990, and was completely revised incorporating the earlier updates in February 1996.

Among the issues that shaped debate over the Computer Security Act was the role of the National Security Agency (NSA) versus NIST in developing technical standards and guidelines for Federal computer privacy and security. Congress did not want the national security community (through NSA's role as National Manager for technical computer standards and guidelines) to have too strong a role in establishing the computer standards for civilian agencies. Hence, Congress gave NIST responsibility for developing standards and guidelines for civilian Federal computer systems, drawing upon the technical advice and assistance from NSA.

Other issues included the need for greater training of personnel involved in Federal computer security, and the scope of the legislation in terms of defining a "Federal computer system." The Act defines a Federal computer system not only as a "computer system operated by a Federal agency," but also "operated by a contractor of a Federal agency or other organization processing information (using a computer system) on behalf of the Federal government to accomplish a Federal function," such as state governments disbursing Federal funds.

LEGISLATIVE HISTORY

The Computer Security Enhancement Act of 1997 was introduced by Representative Sensenbrenner on June 17, 1997, was amended and reported favorably by the House Committee on Science, was passed by the House of Representatives on September 16, 1997, and was referred to the Commerce Committee on September 17, 1997. A Science, Technology, and Space Subcommittee hearing, with Senator Frist presiding, was held on February 10, 1998 at 2:30 p.m.

On October 1, 1998, the Committee met in open executive session and, by a voice vote, ordered H.R. 1903 to be reported without amendment.

SUMMARY OF MAJOR PROVISIONS

The reported bill updates the Computer Security Act to take into account the evolution of computer networks and their use by both the Federal government and the private sector. Specifically, H.R. 1903:

1. Requires NIST to encourage the acquisition of commercial off-the-shelf (COTS) products to meet civilian agency computer security needs. This measure should reduce the cost and improve the availability of computer security technologies for Federal agencies;

2. Enhances the role of the independent Computer System Security and Privacy Advisory Board in NIST's decision-making process by requiring the Board, which is made up of representatives from industry, Federal agencies and other external organizations, to make formal recommendations regarding proposed security standards and provide guidance to NIST on emerging computer security issues;

3. Clarifies that NIST standards and guidelines are to be used for the acquisition of computer security technologies for the Federal government's computer systems containing unclassified information and are not intended as restrictions on the production or use of encryption by the private sector;

4. Updates the Computer Security Act by including references to computer networking which has become an increasingly important component of the Federal government information technology system;

5. Establishes a new computer science fellowship program for graduate and undergraduate students studying computer security. The bill sets aside $250,000 for the first year and $500,000 for the second year, to enable NIST to finance computer security fellowships under an existing NIST grant program;

6. Requires the National Research Council (NRC) to conduct a study to assess the desirability of public key infrastructures. The NRC would also research the technologies required for the establishment of such key infrastructures;

7. Requires the Under Secretary of Commerce for Technology to actively promote the use of technologies by the Federal Government that will enhance the security of Federal communications networks and information in electronic form; to establish a clearinghouse of information available to the public on information security threats; and to promote development of a market driven consensus standards-based infrastructure that will enable more widespread use of encryption technologies for confidentiality and authentication; and

8. Establishes a National Panel for Digital Signatures for the purpose of exploring all relevant factors associated with the development of a national digital signature infrastructure based on uniform standards and of developing model practices and standards associated with certification authorities.

ESTIMATED COSTS

In accordance with paragraph 11(a) of rule XXVI of the Standing Rules of the Senate and section 403 of the Congressional Budget Act of 1974, the Committee provides the following cost estimate, prepared by the Congressional Budget Office:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, October 8. 1998.

Hon. JOHN MCCAIN,
Chairman, Committee on Commerce, Science and Transportation, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 1903, the Computer Security Enhancement Act of 1998.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Hadley.

Sincerely,

JUNE E. O'NEILL, *Director.*

Enclosure.

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

H.R. 1903—Computer Security Enhancement Act of 1997

Summary: H.R. 1903 would direct the National Institute of Standards and Technology (NIST), located in the Department of Commerce, to develop policies to improve computer security for federal computer systems. CBO estimates that implementing the act would cost $13 million over the 1999–2003 period, assuming appropriation of the necessary amount.

H.R. 1903 would authorize the appropriation of about $2 million to NIST to (1) enable the Computer System Security and Privacy Advisory Board (CSSPAB) administered by NIST to conduct pubic forums to identify emerging issues related to computer security, (2) contract for a study by the National Research Council on computer security issues, and (3) award computer security fellowships. In addition, CBO estimates that implementing other provisions of the legislation would require expenditures of about $11 million over the 1999–2003 period.

H.R. 1903 would not affect direct spending or receipts; therefore, pay-as-you go procedures would not apply. H.R. 1903 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would not affect the budgets of state, local, or tribal governments.

Estimated cost to the Federal Government: For the purposes of this estimate, CBO assumes that H.R. 1903 will be enacted near the start of fiscal year 1999, and that the estimated amounts necessary to implement the act will be appropriated for each fiscal year. Outlays have been projected on the basis of historical spending patterns for NIST and information provided by the agency. The estimated budgetary impact of H.R. 1903 is shown in the following table.

	By fiscal years, in millions of dollars—				
	1999	2000	2001	2002	2003
CHANGES IN SPENDING SUBJECT TO APPROPRIATIONS					
Estimated Authorization Level	5	2	2	2	2
Estimated Outlays	4	3	2	2	2

NIST received an appropriation of $571 million for fiscal year 1998, and its 1998 outlays are estimated to be about $617 million.

The costs of this legislation fall within budget function 370 (commerce and housing credit).

Basis of estimate: Based on information from NIST, CBO estimates that enacting H.R. 1903 would result in total costs to the government of about $13 million over the 1999–2003 period. Of that amount, about $2 million is specifically authorized in the act for the activities of the CSSPAB and the National Research Council, as well as for the computer security fellowship program at NIST.

CBO estimates that NIST would need additional appropriations of between $2 million and $3 million in each fiscal year over the 1999–2003 period to implement the remaining provisions of H.R. 1903, including testing computer security products for use by federal agencies, providing information on computer security threats to the public, and establishing a National Panel for Digital Signatures.

H.R. 1903 directs that the sums necessary to implement this act, including the $2 million explicitly authorized in it, should be derived from amounts authorized to be appropriated in H.R. 1274, the National Institute of Standards and Technology Authorization Act of 1997. That legislation has been passed by the House of Representatives but has not yet been enacted into law.

Pay-as-you-go considerations: None.

Intergovernmental and private-sector impact: H.R. 1903 contains no intergovernmental or private-sector mandates as defined in UMRA and would not affect the budgets of state, local, or tribal governments.

Previous CBO estimate: On August 12, 1997, CBO transmitted a cost estimate for H.R. 1903, as ordered reported by the House Committee on Science on July 29, 1997. That version of the legislation would require NIST to evaluate commercial encryption products subject to export restrictions, at an estimated cost of about $5 million a year. CBO estimated five-year costs of $35 million for the House-reported bill, as compared to the five-year costs of $13 million for the Senate version.

Estimate prepared by: Mark Hadley.

Estimate approved by: Robert A. Sunshine, Deputy Assistant Director for Budget Analysis.

REGULATORY IMPACT STATEMENT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee provides the following evaluation of the regulatory impact of the legislation, as reported:

NUMBER OF PERSONS COVERED

The Committee believes that the bill will not subject any individuals or businesses affected by the bill to any additional regulation.

ECONOMIC IMPACT

This legislation will not have an adverse economic impact on the Nation.

PRIVACY

This legislation will not have an adverse impact on the privacy of individuals. It is expected that the legislation will increase the level of security in Federal computer systems which may contain information on individuals and businesses.

PAPERWORK

This legislation will not increase the paperwork requirements for private individuals or businesses.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title

This section cites the short title of the bill as the "Computer Security Enhancement Act of 1997."

Section 2. Findings and purposes

This section details the findings and purposes of the bill.

Section 3. Voluntary standards for public key management infrastructure

This section amends section 20 of the NIST Act by authorizing NIST to assist, upon request from the private sector, in establishing voluntary interoperable standards, guidelines, and associated methods and techniques to facilitate and expedite the establishment of non-Federal public key management infrastructures that can be used to communicate with and conduct transactions with the Federal Government.

Section 4. Security of Federal computers and networks

This section further amends section 20 of the NIST Act by authorizing NIST to:

1. provide guidance and assistance to Federal agencies in the protection of interconnected computer systems and coordinate Federal response efforts related to unauthorized access to Federal computer systems; and
2. perform evaluations and tests of information technologies to assess security vulnerabilities and of commercially available security products for their suitability for use by Federal agencies for protecting sensitive information in computer systems.

Section 5. Computer security implementation

This section makes another amendment to section 20 of the NIST Act, to specify the approaches to be taken by NIST in carrying out its existing responsibilities for developing standards and guidelines for the security and privacy of sensitive information in Federal computer systems. Specifically, NIST would be required to emphasize technology-neutral policy guidelines, and must actively promote commercially available products to provide for the security and privacy requirements of Federal computer systems. Also, NIST is required to participate in implementations of encryption technologies to develop necessary standards and guidelines for Federal computer systems, including assessing the desirability of and the

costs associated with establishing and managing a key recovery infrastructure for Federal Government information.

Section 6. Computer security review, public meetings, and information

This section also amends section 20 of the NIST Act, requiring NIST to solicit recommendations of the Computer System Security and Privacy Advisory Board regarding standards and guidelines that are under consideration for submittal to the Secretary of Commerce for promulgation as regulations and include such recommendations with any subsequent submission to the Secretary. Funds are also authorized for the Board ($1,000,000 for FY 1998 and $1,030,000 for FY 1999) to enable it to act as a forum for public discussion on emerging issues related to computer security, privacy and cryptography. The Board is authorized to convene public meetings on those subjects and to publish reports, digests, and summaries for public distribution.

Section 7. Limitation on participation in requiring encryption standards

This section amends section 20 of the NIST Act by prohibiting NIST from promulgating, enforcing, or otherwise adopting standards, or carrying out activities or policies, for the Federal establishment of encryption standards required for use in computer systems other than Federal Government computer systems.

Section 8. Miscellaneous amendments

This section makes technical and conforming amendments to section 20 of the NIST Act, as well as a language modification which reasserts NIST's role as the lead agency for handling standards for civilian agency computer security.

Section 9. Federal computer system security training

This section amends section 5(b) of the Computer Security Act of 1987 by adding an emphasis on protecting sensitive information in Federal databases and Federal computer sites that are accessible through public networks.

Section 10. Computer Security Fellowship Program

This section authorizes funds, subject to provisions of section 18 of the NIST Act, for the Director of NIST to provide fellowships for research on computer security to students at institutions of higher learning ($250,000 for FY 1998 and $500,000 FY 1999).

Section 11. Study of public key infrastructure by the National Research Council

This section requires the Secretary of Commerce, within 90 days of enactment of this bill, to enter into a contract with the National Research Council of the National Academy of Sciences to conduct a study of public key infrastructures for use by individuals, businesses, and government. All Federal agencies are required to cooperate fully with the National Research Council in conducting the study, including access by properly cleared individuals to classified information if necessary. The Secretary is required to transmit the

report, unclassified, by the National Research Council to the Committee on Science of the House of Representatives and the Committee on Commerce, Science and Transportation of the Senate. $450,000 is authorized for FY 1998 and is to remain available until expended.

Section 12. Promotion of national information security

This section requires the Under Secretary of Commerce for Technology to:

1. promote the more widespread use of applications of cryptography and associated technologies to enhance the security of the Nation's information infrastructure;
2. establish a central clearinghouse for the collection by the Federal Government and dissemination to the public of information to promote awareness of information security threats; and
3. promote the development of the national, standards-based infrastructure needed to support commercial and private uses of encryption technologies for confidentiality and authentication.

Section 13. Digital signature infrastructure

This section requires the Under Secretary of Commerce for Technology to establish a National Policy Panel for Digital Signatures. Its purpose would be to explore all relevant factors associated with the development of a national digital signature infrastructure based on uniform standards that will enable the widespread availability and use of digital signature systems. The panel would be composed of nongovernmental and governmental technical and legal experts on the implementation of digital signatures, individuals from companies offering digital signature products and services, state officials, including offices from States, and representative individuals from the interested public. The Technology Administration of the Department of Commerce shall appoint the National Policy Panel and provide necessary administrative support.

Section 14. Source of authorizations

This section indicates that amounts authorized to be appropriated by this bill are from amounts authorized by the NIST Authorization Act of 1997.

CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, 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 material is printed in italic, existing law in which no change is proposed is shown in roman):

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT

[15 U.S.C. 278G-3]

SEC. 20. (a) The Institute 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(9) 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(9) 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 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

(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 Institute 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) upon request from the private sector, to assist in establishing voluntary interoperable standards, guidelines, and associated methods and techniques to facilitate and expedite the establishment of non-Federal management infrastructures for public keys that can be used to communicate with and conduct transactions with the Federal Government;

[(2)] *(3)* as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

[(3)] *(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 provide guidance and assistance to Federal agencies in the protection of interconnected computer systems and to coordinate Federal response efforts related to unauthorized access to Federal computer systems;

(6) to perform evaluations and tests of—

(A) information technologies to assess security vulnerabilities; and

(B) commercially available security products for their suitability for use by Federal agencies for protecting sensitive information in computer systems;

[(4)] *(7)* 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

[(5)] *(8)* 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) *to the extent that such coordination will improve computer security and to the extent necessary for improving such security for Federal computer systems—*

(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) In carrying out subsection (a)(3), the Institute shall—

(1) emphasize the development of technology-neutral policy guidelines for computer security practices by the Federal agencies;

(2) actively promote the use of commercially available products to provide for the security and privacy of sensitive information in Federal computer systems; and

(3) participate in implementations of encryption technologies in order to develop required standards and guidelines for Federal computer systems, including assessing the desirability of and the costs associated with establishing and managing key recovery infrastructures for Federal Government information.

(d)(1) The Institute shall solicit the recommendations of the Computer System Security and Privacy Advisory Board, established by section 21, regarding standards and guidelines that are being considered for submittal to the Secretary of Commerce in accordance with subsection (a)(4). No standards or guidelines shall be submitted to the Secretary prior to the receipt by the Institute of the

Board's written recommendations. The recommendations of the Board shall accompany standards and guidelines submitted to the Secretary.

(2) There are authorized to be appropriated to the Secretary of Commerce $1,000,000 for fiscal year 1998 and $1,030,000 for fiscal year 1999 to enable the Computer System Security and Privacy Advisory Board, established by section 21, to identify emerging issues related to computer security, privacy, and cryptography and to convene public meetings on those subjects, receive presentations, and publish reports, digests, and summaries for public distribution on those subjects.

[(c)] *(e)* For the purposes of—

(1) developing standards and guidelines for the protection of sensitive information in Federal computer systems under subsections (a)(1) and (a)(3), and

(2) performing research and conducting studies under subsection [(b)(5),] *(b)(8),*

the Institute [shall draw upon] *may 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)] *(f)* 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 *and computer networks*;

(ii) ancillary equipment;

(iii) software, firmware, and similar procedures;

(iv) services, including support services; and

(v) related resources;

(2) the term "Federal computer system" 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;

(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.

(g) The Institute shall not promulgate, enforce, or otherwise adopt standards, or carry out activities or policies, for the Federal establishment of encryption standards required for use in computer systems other than Federal Government computer systems.

* * * * * * *

COMPUTER SECURITY ACT OF 1987

SEC. 5. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.

(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 oration 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.] *practices; and*

(3) to include emphasis on protecting sensitive information in Federal databases and Federal computer sites that are accessible through public networks.

(c) REGULATIONS.—Within six months after the date of 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.

○

Document No. 27