I

107TH CONGRESS
1ST SESSION

H. R. 1259

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.

IN THE HOUSE OF REPRESENTATIVES

MARCH 28, 2001

Mrs. MORELLA (for herself, Mr. GORDON, Mr. BOEHLERT, Mr. BARCIA, Mr. EHLERS, Mr. ETHERIDGE, and Mr. GUTKNECHT) introduced the following bill; which was referred to the Committee on Science

---

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.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Computer Security Enhancement Act of 2001''.

SEC. 2. FINDINGS AND PURPOSES.

(a) FINDINGS.—The Congress finds the following:

★

(1) The National Institute of Standards and Technology has responsibility for developing standards and guidelines needed to ensure the cost-effective security and privacy of sensitive information in Federal computer systems.

(2) The Federal Government has an important role in ensuring the protection of sensitive, but unclassified, information controlled by Federal agencies.

(3) Technology that is based on the application of cryptography exists and can be readily provided by private sector companies to ensure the confidentiality, authenticity, and integrity of information associated with public and private activities.

(4) The development and use of encryption technologies by industry should be driven by market forces rather than by Government imposed requirements.

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

(1) reinforce the role of the National Institute of Standards and Technology in ensuring the security of unclassified information in Federal computer systems; and

(2) promote technology solutions based on private sector offerings to protect the security of Federal computer systems.

SEC. 3. SECURITY OF FEDERAL COMPUTERS AND NETWORKS.

Section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)) is amended—

(1) by redesignating paragraphs (4) and (5) as paragraphs (7) and (8), respectively; and

(2) by inserting after paragraph (3) the following new paragraphs:

''(4) except for national security systems, as defined in section 5142 of Public Law 104-106 (40 U.S.C. 1452), to provide guidance and assistance to Federal agencies for protecting the security and privacy of sensitive information in interconnected Federal computer systems, including identification of significant risks thereto;

''(5) to promote compliance by Federal agencies with existing Federal computer information security and privacy guidelines;

''(6) in consultation with appropriate Federal agencies, assist Federal response efforts related to unauthorized access to Federal computer systems;''.

SEC. 4. COMPUTER SECURITY IMPLEMENTATION.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is further amended—

(1) by redesignating subsections (c) and (d) as subsections (e) and (f), respectively; and

(2) by inserting after subsection (b) the following new subsection:

''(c)(1) In carrying out subsection (a)(2) and (3), the Institute shall—

''(A) emphasize the development of technology-neutral policy guidelines for computer security and electronic authentication practices by the Federal agencies;

''(B) promote the use of commercially available products, which appear on the list required by paragraph (2), to provide for the security and privacy of sensitive information in Federal computer systems;

''(C) develop qualitative and quantitative measures appropriate for assessing the quality and effectiveness of information security and privacy programs at Federal agencies;

''(D) perform evaluations and tests at Federal agencies to assess existing information security and privacy programs;

''(E) promote development of accreditation procedures for Federal agencies based on the measures developed under subparagraph (C);

''(F) if requested, consult with and provide assistance to Federal agencies regarding the selection by agencies of security technologies and products and the implementation of security practices; and

''(G)(i) develop uniform testing procedures suitable for determining the conformance of commercially available security products to the guidelines and standards developed under subsection (a)(2) and (3);

''(ii) establish procedures for certification of private sector laboratories to perform the tests and evaluations of commercially available security products developed in accordance with clause (i); and

''(iii) promote the testing of commercially available security products for their conformance with guidelines and standards developed under subsection (a)(2) and (3).

''(2) The Institute shall maintain and make available to Federal agencies and to the public a list of commercially available security products that have been tested by private sector laboratories certified in accordance with procedures established under paragraph (1)(G)(ii), and that

have been found to be in conformance with the guidelines and standards developed under subsection (a)(2) and (3).

''(3) The Institute shall annually transmit to the Congress, in an unclassified format, a report containing—

''(A) the findings of the evaluations and tests of Federal computer systems conducted under this section during the 12 months preceding the date of the report, including the frequency of the use of commercially available security products included on the list required by paragraph (2);

''(B) the planned evaluations and tests under this section for the 12 months following the date of the report; and

''(C) any recommendations by the Institute to Federal agencies resulting from the findings described in subparagraph (A), and the response by the agencies to those recommendations.''.

SEC. 5. COMPUTER SECURITY REVIEW, PUBLIC MEETINGS, AND INFORMATION.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), as amended by this Act, is further amended by inserting after subsection (c), as added by section 4 of this Act, the following new subsection:

''(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 in accordance with subsection (a)(4). The recommendations of the Board shall accompany standards and guidelines submitted to the Secretary.

''(2) There are authorized to be appropriated to the Secretary $1,030,000 for fiscal year 2002 and $1,060,000 for fiscal year 2003 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.''.

SEC. 6. LIMITATION ON PARTICIPATION IN REQUIRING ENCRYPTION AND ELECTRONIC AUTHENTICATION STANDARDS.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), as amended by this Act, is further amended by adding at the end the following new subsection:

''(g) The Institute shall not promulgate, enforce, or otherwise adopt standards or policies for the Federal es-

tablishment of encryption and electronic authentication standards required for use in computer systems other than Federal Government computer systems.''.

SEC. 7. MISCELLANEOUS AMENDMENTS.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), as amended by this Act, is further amended—

(1) in subsection (b)(8), as so redesignated by section 3(1) of this Act, by inserting ''to the extent that such coordination will improve computer security and to the extent necessary for improving such security for Federal computer systems'' after ''Management and Budget)'';

(2) in subsection (e), as so redesignated by section 4(1) of this Act, by striking ''shall draw upon'' and inserting in lieu thereof ''may draw upon'';

(3) in subsection (e)(2), as so redesignated by section 4(1) of this Act, by striking ''(b)(5)'' and inserting in lieu thereof ''(b)(7)''; and

(4) in subsection (f)(1)(B)(i), as so redesignated by section 4(1) of this Act, by inserting ''and computer networks'' after ''computers''.

SEC. 8. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.

Section 5(b) of the Computer Security Act of 1987 (40 U.S.C. 759 note) is amended—

(1) by striking ''and'' at the end of paragraph (1);

(2) by striking the period at the end of paragraph (2) and inserting in lieu thereof ''; and''; and

(3) by adding at the end the following new paragraph:

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

SEC. 9. COMPUTER SECURITY FELLOWSHIP PROGRAM.

There are authorized to be appropriated to the Secretary of Commerce $500,000 for fiscal year 2002 and $500,000 for fiscal year 2003 for the Director of the National Institute of Standards and Technology for fellowships, subject to the provisions of section 18 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–1), to support students at institutions of higher learning in computer security. Amounts authorized by this section shall not be subject to the percentage limitation stated in such section 18.

SEC. 10. STUDY OF ELECTRONIC AUTHENTICATION TECHNOLOGIES BY THE NATIONAL RESEARCH COUNCIL.

(a) REVIEW BY NATIONAL RESEARCH COUNCIL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Commerce shall enter into a contract with the National Research Council of the National Academy of Sciences to conduct a study of electronic authentication technologies for use by individuals, businesses, and government.

(b) CONTENTS.—The study referred to in subsection (a) shall—

(1) assess technology needed to support electronic authentication technologies;

(2) assess current public and private plans for the deployment of electronic authentication technologies;

(3) assess interoperability, scalability, and integrity of private and public entities that are elements of electronic authentication technologies; and

(4) address such other matters as the National Research Council considers relevant to the issues of electronic authentication technologies.

(c) INTERAGENCY COOPERATION WITH STUDY.—All agencies of the Federal Government shall cooperate fully with the National Research Council in its activities in car-

rying out the study under this section, including access by properly cleared individuals to classified information if necessary.

(d) REPORT.—Not later than 18 months after the date of the enactment of this Act, the Secretary of Commerce shall transmit to the Committee on Science of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report setting forth the findings, conclusions, and recommendations of the National Research Council for public policy related to electronic authentication technologies for use by individuals, businesses, and government. The National Research Council shall not recommend the implementation or application of a specific electronic authentication technology or electronic authentication technical specification for use by the Federal Government. Such report shall be submitted in unclassified form.

(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary of Commerce $450,000 for fiscal year 2002, to remain available until expended, for carrying out this section.

SEC. 11. PROMOTION OF NATIONAL INFORMATION SECURITY.

The Under Secretary of Commerce for Technology shall—

(1) promote an increased use of security techniques, such as risk assessment, and security tools, such as cryptography, to enhance the protection of the Nation's information infrastructure;

(2) establish a central repository of information for dissemination to the public to promote awareness of information security vulnerabilities and risks; and

(3) in a manner consistent with section 12(d) of the National Technology Transfer and Advancement Act of 1995 (15 U.S.C. 272 nt), promote the development of national standards-based infrastructures needed to support government, commercial, and private uses of encryption technologies for confidentiality and authentication.

SEC. 12. ELECTRONIC AUTHENTICATION INFRASTRUCTURES.

(a) ELECTRONIC AUTHENTICATION INFRASTRUCTURES.—

(1) TECHNOLOGY-NEUTRAL GUIDELINES AND STANDARDS.—Not later than 18 months after the date of the enactment of this Act, the Director, in consultation with industry and appropriate Federal agencies, shall develop technology-neutral guidelines and standards, or adopt existing technology-neutral industry guidelines and standards, for electronic au-

thentication infrastructures to be made available to Federal agencies so that such agencies may effectively select and utilize electronic authentication technologies in a manner that is—

(A) adequately secure to meet the needs of those agencies and their transaction partners; and

(B) interoperable, to the maximum extent possible.

(2) ELEMENTS.—The guidelines and standards developed under paragraph (1) shall include—

(A) protection profiles for cryptographic and noncryptographic methods of authenticating identity for electronic authentication products and services;

(B) a core set of interoperability specifications for the use of electronic authentication products and services in electronic transactions between Federal agencies and their transaction partners; and

(C) validation criteria to enable Federal agencies to select cryptographic electronic authentication products and services appropriate to their needs.

(3) REVISIONS.—The Director shall periodically review the guidelines and standards developed under paragraph (1) and revise them as appropriate.

(b) LISTING OF PRODUCTS.—Not later than 30 months after the date of the enactment of this Act, and thereafter, the Director shall maintain and make available to Federal agencies a nonmandatory list of commercially available electronic authentication products, and other such products used by Federal agencies, evaluated as conforming with the guidelines and standards developed under subsection (a).

(c) SPECIFICATIONS FOR ELECTRONIC CERTIFICATION AND MANAGEMENT TECHNOLOGIES.—

(1) SPECIFICATIONS.—The Director shall, as appropriate, establish core specifications for particular electronic certification and management technologies, or their components, for use by Federal agencies.

(2) EVALUATION.—The Director shall advise Federal agencies on how to evaluate the conformance with the specifications established under paragraph (1) of electronic certification and management technologies, developed for use by Federal agencies or available for such use.

(3) MAINTENANCE OF LIST.—The Director shall maintain and make available to Federal agencies a list of electronic certification and management technologies evaluated as conforming to the specifications established under paragraph (1).

(d) REPORTS.—Not later than 18 months after the date of the enactment of this Act, and annually thereafter, the Director shall transmit to the Congress a report that includes—

(1) a description and analysis of the utilization by Federal agencies of electronic authentication technologies; and

(2) a description and analysis regarding the problems Federal agencies are having, and the progress such agencies are making, in implementing electronic authentication infrastructures.

(e) DEFINITIONS.—For purposes of this section—

(1) the term ''electronic authentication'' means cryptographic or noncryptographic methods of authenticating identity in an electronic communication;

(2) the term ''electronic authentication infrastructure'' means the software, hardware, and personnel resources, and the procedures, required to effectively utilize electronic authentication technologies;

(3) the term ''electronic certification and management technologies'' means computer systems, including associated personnel and procedures, that enable individuals to apply electronic authentication to electronic information; and

(4) the term ''protection profile'' means a list of security functions and associated assurance levels used to describe a product.

SEC. 13. SOURCE OF AUTHORIZATIONS.

There are authorized to be appropriated to the Secretary of Commerce $7,000,000 for fiscal year 2002 and $8,000,000 for fiscal year 2003, for the National Institute of Standards and Technology to carry out activities authorized by this Act for which funds are not otherwise specifically authorized to be appropriated by this Act.

○