.....

(Original Signature of Member)

106TH CONGRESS
1ST SESSION

H. R. _____

IN THE HOUSE OF REPRESENTATIVES

Mr. SENSENBRENNER (for himself, Mr. GORDON, and Mrs. MORELLA) introduced the following bill; which was referred to the Committee on _____

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 1999''.

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 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. VOLUNTARY STANDARDS FOR PUBLIC KEY MANAGEMENT INFRASTRUCTURE.

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 (2), (3), (4), and (5) as paragraphs (3), (4), (7), and (8), respectively; and

(2) by inserting after paragraph (1) the following new paragraph:

''(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;''.

SEC. 4. 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)), as amended by section 3 of this Act, is further amended by inserting

after paragraph (4), as so redesignated by section 3(1) of this Act, the following new paragraphs:

''(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;''.

SEC. 5. 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) 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.''.

SEC. 6. 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 5 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). 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 $1,000,000 for fiscal year 2000 and $1,030,000 for fiscal year 2001 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. 7. LIMITATION ON PARTICIPATION IN REQUIRING ENCRYPTION 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 carry out activities or policies, for the Federal establishment of encryption standards

required for use in computer systems other than Federal Government computer systems.''.

SEC. 8. 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 5(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 5(1) of this Act, by striking ''(b)(5)'' and inserting in lieu thereof ''(b)(8)''; and

(4) in subsection (f)(1)(B)(i), as so redesignated by section 5(1) of this Act, by inserting ''and computer networks'' after ''computers''.

SEC. 9. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.

Section 5(b) of the Computer Security Act of 1987 (49 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. 10. COMPUTER SECURITY FELLOWSHIP PROGRAM.

There are authorized to be appropriated to the Secretary of Commerce $250,000 for fiscal year 2000 and $500,000 for fiscal year 2001 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. 11. STUDY OF PUBLIC KEY INFRASTRUCTURE 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 public key infrastructures for use by individuals, businesses, and government.

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

(1) assess technology needed to support public key infrastructures;

(2) assess current public and private plans for the deployment of public key infrastructures;

(3) assess interoperability, scalability, and integrity of private and public entities that are elements of public key infrastructures;

(4) make recommendations for Federal legislation and other Federal actions required to ensure the national feasibility and utility of public key infrastructures; and

(5) address such other matters as the National Research Council considers relevant to the issues of public key infrastructure.

(c) INTERAGENCY COOPERATION WITH STUDY.—All agencies of the Federal Government shall cooperate fully with the National Research Council in its activities in carrying 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 public key infrastructures for use by individuals, businesses, and 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 2000, to remain available until expended, for carrying out this section.

SEC. 12. PROMOTION OF NATIONAL INFORMATION SECURITY.

The Under Secretary of Commerce for Technology shall—

(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.

SEC. 13. ELECTRONIC AUTHENTICATION INFRASTRUCTURE.

(a) ELECTRONIC AUTHENTICATION INFRASTRUCTURE.—

(1) GUIDELINES AND STANDARDS.—Not later than 1 year after the date of the enactment of this Act, the Director, in consultation with industry, shall develop electronic authentication infrastructure guidelines and standards for use by Federal agencies to enable those agencies to effectively utilize electronic authentication technologies in a manner that is—

(A) sufficiently 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) minimum interoperability specifications for the Federal acquisition of electronic authentication products and services; and

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

(3) COORDINATION WITH NATIONAL POLICY PANEL.—The Director shall ensure that the development of guidelines and standards with respect to cryptographic electronic authentication products and services under this subsection is carried out in coordination with the efforts of the National Policy Panel for Digital Signatures under subsection (e).

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

(b) VALIDATION OF PRODUCTS.—Not later than 1 year after the date of the enactment of this Act, and there-

after, the Director shall maintain and make available to Federal agencies and to the public a 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) ELECTRONIC CERTIFICATION AND MANAGEMENT SYSTEMS.—

(1) CRITERIA.—Not later than 1 year after the date of the enactment of this Act, the Director shall establish minimum technical criteria for the use by Federal agencies of electronic certification and management systems.

(2) EVALUATION.—The Director shall establish a program for evaluating the conformance with the criteria established under paragraph (1) of electronic certification and management systems, 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 systems evaluated as conforming to the criteria 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;

(2) an evaluation of the extent to which Federal agencies' electronic authentication infrastructures conform to the guidelines and standards developed under subsection (a)(1);

(3) an evaluation of the extent to which Federal agencies' electronic certification and management systems conform to the criteria established under subsection (c)(1);

(4) the list described in subsection (c)(3); and

(5) evaluations made under subsection (b).

(e) NATIONAL POLICY PANEL FOR DIGITAL SIGNATURES.—

(1) ESTABLISHMENT.—Not later than 90 days after the date of the enactment of this Act, the Under Secretary shall establish a National Policy Panel for Digital Signatures. The Panel shall be composed of government, academic, and industry technical and legal experts on the implementation of digital signature technologies, State officials, including officials from States which have enacted laws

recognizing the use of digital signatures, and representative individuals from the interested public.

(2) RESPONSIBILITIES.—The Panel shall serve as a forum for exploring all relevant factors associated with the development of a national digital signature infrastructure based on uniform guidelines and standards to enable the widespread availability and use of digital signature systems. The Panel shall develop—

(A) model practices and procedures for certification authorities to ensure the accuracy, reliability, and security of operations associated with issuing and managing digital certificates;

(B) guidelines and standards to ensure consistency among jurisdictions that license certification authorities; and

(C) audit procedures for certification authorities.

(3) COORDINATION.—The Panel shall coordinate its efforts with those of the Director under subsection (a).

(4) ADMINISTRATIVE SUPPORT.—The Under Secretary shall provide administrative support to enable the Panel to carry out its responsibilities.

(5) REPORT.—Not later than 1 year after the date of the enactment of this Act, the Under Secretary shall transmit to the Congress a report containing the recommendations of the Panel.

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

(1) the term ''certification authorities'' means issuers of digital certificates;

(2) the term ''digital certificate'' means an electronic document that binds an individual's identity to the individual's key;

(3) the term ''digital signature'' means a mathematically generated mark utilizing key cryptography techniques that is unique to both the signatory and the information signed;

(4) the term ''digital signature infrastructure'' means the software, hardware, and personnel resources, and the procedures, required to effectively utilize digital certificates and digital signatures;

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

(6) the term ''electronic authentication infrastructure'' means the software, hardware, and personnel resources, and the procedures, required to ef-

fectively utilize electronic authentication technologies;

(7) the term ''electronic certification and management systems'' means computer systems, including associated personnel and procedures, that enable individuals to apply unique digital signatures to electronic information;

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

(9) the term ''Under Secretary'' means the Under Secretary of Commerce for Technology.

SEC. 14. SOURCE OF AUTHORIZATIONS.

There are authorized to be appropriated to the Secretary of Commerce $3,000,000 for fiscal year 2000 and $4,000,000 for fiscal year 2001, 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.