106TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
106–876

COMPUTER SECURITY ENHANCEMENT ACT OF 2000

SEPTEMBER 21, 2000.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. SENSENBRENNER, from the Committee on Science, submitted the following

REPORT

[To accompany H.R. 2413]

[Including cost estimate of the Congressional Budget Office]

The Committee on Science, to whom was referred the bill (H.R. 2413) 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, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

79–006

I. AMENDMENT

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Security Enhancement Act of 2000".

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. 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), (8), and (9), 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) 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;

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

"(7) in consultation with appropriate Federal agencies, assist Federal response efforts related to unauthorized access to Federal 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)(1) In carrying out subsection (a)(2) and (3), the Institute shall—

"(A) emphasize the development of technology-neutral policy guidelines for computer security 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. 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). 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 2001 and $1,060,000 for fiscal year 2002 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)(9), 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 (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. 10. COMPUTER SECURITY FELLOWSHIP PROGRAM.

There are authorized to be appropriated to the Secretary of Commerce $500,000 for fiscal year 2001 and $500,000 for fiscal year 2002 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 2001, 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 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) promote the development of the national, standards-based infrastructure needed to support government, 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 18 months after the date of the enactment of this Act, the Director, in consultation with industry and appropriate Federal agencies, shall develop electronic authentication infrastructure guidelines and standards for use by Federal agencies to assist those agen-

cies to 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 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 consultation with the National Policy Panel for Digital Signatures established under subsection (e).

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

(b) LISTING OF VALIDATED 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 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) 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) an evaluation of the extent to which Federal agencies' electronic authentication infrastructures conform to the guidelines and standards developed under subsection (a)(1).

(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 effectively utilize electronic authentication technologies;

(7) the term "electronic certification and management technologies" 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 $7,000,000 for fiscal year 2001 and $8,000,000 for fiscal year 2002, 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.

II. PURPOSE OF THE BILL

The purpose of the bill is to update the Computer Security Act of 1987 to improve computer security for federal civilian agencies and the private sector.

III. BACKGROUND AND NEED FOR THE LEGISLATION

The Computer Security Act of 1987 gave authority over computer and communication security standards in federal civilian agencies to NIST. The Computer Security Enhancement Act of 2000 strengthens that authority and directs funds to implement practices and procedures which will ensure that the federal standards setting process remains open to public input and analysis and that will provide guidance and assistance on protection of electronic information to federal civilian agencies. H.R. 2413 promotes open and public discussion, as well as the use of commercially available products to meet the information security needs of the federal civilian agencies.

Since 1993, the General Accounting Office (GAO) has issued over 35 reports describing serious information security weaknesses at major federal agencies. In 1999, GAO reported that during the previous 2 years serious information security control weaknesses had been reported for most of the federal agencies. Recently, GAO gave the federal government an overall grade of D minus for its computer security efforts.

Much has changed in the years since the Computer Security Act of 1987 was enacted. The proliferation of networked systems, the Internet, and web access are just a few of the dramatic advances

in information technology that have occurred. The Computer Security Enhancement Act of 2000 addresses these changes and provides for greater security for the federal civilian agencies that base their procurement decisions for computer security hardware and software on NIST standards. H.R. 2413 also promotes the use of commercially available products and encourages an open exchange of information between NIST and the private sector. This renewed emphasis on open discussion should help facilitate better security in all communities.

IV. Summary of Hearings

On September 30, 1999, the Subcommittee on Technology held a hearing to review H.R. 2413, the Computer Security Enhancement Act of 2000, legislation introduced by Chairman Sensenbrenner, Representatives Morella and Gordon.

Witnesses included Mr. Raymond Kammer, Director, National Institute of Standards and Technology; Mr. Keith Rhodes, Director, Office of Computer and Information, Technology Assessment, U.S. General Accounting Office; Mr. Harris Miller, President, Information Technology Association of America; and Dr. George Trubow, Professor and Director, Center for Information Technology and Privacy Law, The John Marshall Law School and Member, Computer System Security and Privacy Advisory Board (CSSPAB), NIST.

Mr. Kammer testifying on behalf of the National Institute of Standards and Technology, stated that NIST's computer security program focuses on standards and guidelines, public key infrastructure and security research. Mr. Kammer noted that the President has recently requested an additional $39M in FY 2000 for initiatives proposed to protect critical infrastructure, of which $5M would be for NIST to establish an Expert Review Team to assist Government-wide agencies in adhering to Federal computer security requirements. NIST would consult with OMB and NSA on the team's plan to protect computer security for Federal agencies. Two million would fund a 15 member team responsible for helping agencies identify vulnerabilities, plan secure systems and implement critical infrastructure plans. Three million would establish an operational fund at NIST for computer security projects among Federal agencies. Projects would include independent vulnerability assessments, computer intrusion drill and emergency funds to cover security fixes for systems identified to have unacceptable risks.

Mr. Rhodes, testifying on behalf of General Accounting Office (GAO), stated that H.R. 2413 aims to reinforce the role of NIST, whose mission is to provide guidance and technical assistance to government and industry to protect unclassified information systems. Mr. Rhodes discussed: (1) the urgent need to strengthen computer security across the Federal Government; (2) the current and future privacy concerns with any computer security legislation, (3) GAO's views on the proposed act, and (4) what can be done to further strengthen security program management at federal agencies. According to Rhodes, it is imperative that the Federal Government swiftly implement long-term solutions both at individual agencies and government-wide to protect systems and sensitive data. He noted that the need to protect sensitive data and systems must be weighed against cost, feasibility, privacy and security interests of citizens and private businesses as well as national security and law

enforcement agencies. Without computer security, privacy cannot be assured. Without agreement among users, businesses, law enforcement, national security and other authorities on requirements, there is no way to implement new technology or to establish standards that will be universally accepted. Finally, Mr. Rhodes stated that it is important to ensure that NIST retains the ability to develop security standards for unclassified data and decide which industry standards are appropriate for Federal agencies and that the agencies consistently implement such standards.

Mr. Harris, testifying on behalf of the ITAA, stated that his association and its members support both goals of H.R. 2413, to assist NIST in meeting the computer security needs of Federal agencies and to allow the Federal Government through NIST to harness the ingenuity of the private sector to help address its computer security needs. He noted that computer security solutions should be industry-led. Mr. Harris recognized that great opportunities for collaboration between Federal Government and private industry currently exist and that there is a need for information security computer specialists and additional resources. Finally, Mr. Harris stated there is a need for authentication through digital signatures and a public key infrastructure.

Profesor Trubow, testifying on behalf of the Computer System Security and Privacy Advisory Board (CSSPAB), warned that for the Board to remain effective, it should maintain its role as an advisory board. He noted that it is appropriate for the board to be asked for its advice and wisdom. In his opinion, the board supports the goal of H.R. 2413 to expand NIST's activities in developing and promoting the use of information system security technologies. He noted that attention to privacy must not be overlooked. Finally, Professor Trubow recommended that "privacy" be inserted in the bill in several areas.

On April 15, 1999, the Subcommittee on Technology held a hearing on "The Melissa Virus: Inoculating Our Information Technology from Emerging Threats." The hearing was held to review computer security threats specifically computer viruses.

Witnesses included: Mr. Raymond Kammer, Director, National Institutes of Standards and Technology, Mr. Michael Vatis, Director, National Infrastructure and Protection Center, FBI, Dr. Richard Pethia, Director, CERT Coordination Center, Carnegie Mellon University Software Engineering Institute, and Mr. Keith Rhodes, Technical Director, Office of the Chief Scientist, U.S. General Accounting Office.

Mr. Raymond Kammer, Director, National Institutes of Standards and Technology, testified that the Melissa virus is what is known as a denial of service attack, whereby servers and routers are literally overwhelmed by e-mail. Mr. Kammer stressed that we as a nation must maintain a proper perspective in developing computer security solutions and not target the problem of the moment. Mr. Kammer stated that NIST has taken a broad perspective and that the agency has several initiatives underway to strengthen the IT security infrastructure of the U.S. economy.

Mr. Michael Vatis, Director, National Infrastructure and Protection Center, FBI, testified that the Melissa virus is a macro virus spread through Microsoft Word 97 or Word 2000 e-mail attachments. He explained that the problem with this particular virus

was its ability to spread quickly. Mr. Vatis moved on to state that we are fortunate this virus did not do more damage than it did. However, he added that its occurrence should serve as a wake up call for both the government and the private sector, because the virus exploited known vulnerabilities. Mr. Vatis stated that the notifications and information provided by the NIPC, CERT, and others demonstrated the value of cooperative efforts by the private and government sectors.

Dr. Richard Pethia, Director, CERT Coordination Center, Carnegie Mellon University Software Engineering Institute, stated that the Melissa virus was a warning siren of the increased vulnerability of our networks. He believes that the press acted responsibly in reporting the outbreak. Dr. Pethia presumes that there will be a need in the future for enhanced incident response capability, faster communications, better analytical tools and techniques to solve this problem. He contends that if we have multiple outbreaks that spread at Internet speed, we would not be able to control the virus. He reiterates that real solutions in the long term can only come from improvements in technology. Along with virus-proof software, there is a need to make use of encryption technology in the form of digital signatures so those messages can be authenticated.

Mr. Keith Rhodes, Technical Director, Office of the Chief Scientist, U.S. General Accounting Office testified that the Melissa virus disrupted the operations of thousands of companies and some government agencies, but did not permanently damage systems and did not compromise government data. He discussed the broader implications of the Melissa virus including how quickly the virus proliferated due to the extensive connectivity of today's networks. He believes that the next virus will propagate faster, do more damage and be more difficult to detect and to counter. He also claims that it is imperative that Federal agencies and the government implement long-term solutions to protect systems and sensitive data. Furthermore, Mr. Rhodes is a supporter of the GAO's Information Security Best Practice guides. They offer a framework for agencies to follow. Sustained government-wide leadership is needed to ensure that executives understand risks, monitor agency performs and resolve issues affecting multiple agencies.

On May 10, 2000 the Subcommittee on Technology held a hearing entitled, "The Love Bug Virus: Protecting Lovesick Computers from Malicious Attack." The hearing examined the features of the "love bug" computer virus, explored its impact on the Federal Government and the private sector, and examined possible solutions and preventative actions individuals and organizations should take to prevent emerging threats form impacting information technology systems and networks.

Witnesses included: Mr. Keith Rhodes, Technical Director, Office of the Chief Scientist, U.S. General Accounting Office; Mr. Harris Miller, President, Information Technology Association of America; Ms. Sandra England, Senior Vice President, McAfee—A Network Associates Company; Mr. Peter Tippett, Chief Technology Officer, ICSA.net.

Mr. Keith Rhodes, Technical Director, Office of the Chief Scientist, U.S. General Accounting Office, stated that the world does not practice safe computing. He described how the "I Love You" virus worked. He noted that there were 14 variances of this virus

some even more damaging. The Love Bug hit many large corporations such as AT&T, TWA, Ford and the Washington Post, ABC News, British Parliament, the IMF and at least 14 other United States Federal Agencies. These viruses were spreading faster due to the high dependency on our network systems. Mr. Rhodes claims that there is no silver bullet that will stop the infection of viruses. Therefore, agencies inside and outside the government must increase awareness, ensure that existing controls are operating effectively, ensure that software patches are brought up to date, use automated scanning and testing tools to quickly identify problems and be sure that common vulnerabilities are addressed.

Mr. Harris Miller, President, Information Technology Association of America, testified that cyber crimes are given less priority than other types of crime since there is no actual physical violence. This attitude must change and the government agencies need to make information security a much higher priority. He stated that information sharing is the key challenge. He is working to create an information-sharing mechanism with over 100 IT companies. ITAA will host the first global security summit in Washington, D.C. on October 16 and 17. He hopes to establish the same type of international collaboration that existed with the Y2K bug. ITAA is also working with the Department of Justice on the Cybercitizen Partnership to help promote cyber ethics. In his closing remarks he stated that Cyber-crime must not become an accepted practice.

Ms. Sandra England, Senior Vice President, McAfee—A Network Associates Company testified that the McAfee's Emergency response team, AVERT, immediately responded to the outbreak of the "I Love You" virus. They were able to dispense a cure within a couple hours of its first detection. She went on to add that many viruses are detected on a daily basis and last year alone there were $12 billion in damages due to various viruses. Ms. England claims that even though viruses attack on a more frequent basis, not much is being done to internal policies to respond to these new attacks. The actual cost from the viruses is hard to assess mainly since it is a loss of time and productivity. The anti virus companies alone can not combat this problem. Anti-virus software must be kept up to date, and signature files must be updated faithfully. She agreed that more must be done to stop virus writers and in turn stiffer punishments must be enacted.

Mr. Peter Tippett, Chief Technology Officer, ICSA.net discussed the costs and risks associated with electronic, malicious code, privacy, down time, physical and human related factors. He described ICSA as a new breed of Internet company that provides security assurances services. Mr. Tippett states that every product that ICSA certifies can detect, prevent and recover from every virus that has ever been promulgated. However, after they are installed into companies they become only 30% effective. He suggests better education on how to use such software. He agreed with the other witnesses in stating that stiffer laws must be invoked on those who choose to write these malicious codes. ICSA estimates that 65% of Northern American companies were infected as well as 133,000 desktops.

V. COMMITTEE ACTIONS

On Wednesday, October 20, 1999, the Committee on Science, Subcommittee on Technology convened to mark up H.R. 2413, The Computer Security Enhancement Act of 1999, to enhance the ability of the National Institute of Standards and Technology (NIST) to improve computer security. One amendment was offered at the mark-up. It was adopted by a voice vote.

1. Mrs. Morella and Mr. Barcia offered an en bloc amendment that would require NIST to access existing information security programs at Federal agencies, make recommendations to improve their security, and report to Congress annually on the information security status of Federal agencies.

With a quorum present, Chairwoman Morella moved that H.R. 2413, as amended be reported. The motion was adopted by a voice vote.

On Wednesday, July 26, 2000, the Committee on Science convened to mark up H.R. 2413. An amendment offered by Mrs. Morella and Mr. Barcia was offered and adopted by a voice vote.

1. Mrs. Morella and Mr. Barcia offered an amendment, which consisted of the text of H.R. 2413 as reported by the Subcommittee on Technology. The amendment was agreed to by a voice vote.

With a quorum present, Chairman Sensenbrenner moved that H.R. 2413, as amended be reported. The motion was adopted by a voice vote.

VI. SUMMARY OF MAJOR PROVISIONS OF THE BILL

H.R. 2413, the Computer Security Enhancement Act of 2000 provides for greater security for the federal civilian agencies that base their procurement decisions for computer security hardware and software on NIST standards. The legislation also promotes the use of commercially available products and encourages an open exchange of information between NIST and the private sector. The legislation authorizes a total of $8,980,000 in FY 2001 and $9,560,000 in FY 2002. Specifically, the Computer Security Enhancement Act of 2000:

- Requires NIST to encourage the acquisition of commercial off-the-shelf (COTS) products to meet civilian agency computer security needs. This measures should reduce the costs of computer security technologies for federal agencies.
- 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.
- Clarifies that NIST standards and guidelines are to be used for the acquisition of computer security technologies for the Federal Government and are not intended as restrictions on the production or use of encryption by the private sector.
- 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.

• Establishes a new computer science fellowship program for graduate and undergraduate students studying computer security. The bill sets aside $500,000 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.

• 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 public key infrastructures.

• 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.

• 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. The Department of Commerce shall appoint the National Panel and provide necessary administrative support.

VII. Section-by-Section Analysis (By Title and Section)/ Committee Views

Sec. 1. Short title

Computer Security Enhancement Act of 2000.

Sec. 2. Findings and purposes

Details the findings and purpose of the bill.

Sec. 3. Voluntary standards for public key management infrastructures

Section 20 of the NIST Act is amended 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.

Committee views

Historically, NIST has been most effective when helping the commercial sector, in a consensus process, to establish standards. The Committee supports such efforts, so long as they are fully voluntary and reflect a true consensus process.

Sec. 4. Security of Federal computers and networks

Section 20 of the NIST Act is amended by authorizing NIST to:

(1) provide guidance and assistance to federal agencies in the protection of interconnected computer systems (except for national security systems), including identification of significant risks thereto;

(2) promote compliance by Federal agencies with existing Federal computer information security and privacy guidelines; and,

(3) consult with and assist Federal agencies in response to efforts related to unauthorized access to federal computer systems.

Committee views

The Committee believes it is important that NIST remain the lead agency in securing the information technology infrastructure of federal civilian agencies. NIST must place greater emphasis on its duties in this area. NIST should provide guidance and assistance to federal civilian agencies in helping to secure their information technology systems.

Sec. 5. Computer security implementation.

Section 20 of the NIST Act is amended 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 and for assisting federal agencies in meeting those standards and guidelines. Specifically, NIST must emphasize technology-neutral policy guidelines, must actively promote commercially available products for meeting the security and privacy requirements of federal agencies and provide assistance to agencies in the selection of products; and must develop qualitative and quantitative measures for assessing the effectiveness of agencies' information security and privacy programs, perform evaluations of agencies' security and privacy programs, and promote appropriate accreditation procedures for agencies' programs. In addition, NIST is required to develop uniform procedures for determining the effectiveness of commercially available security products; establish procedures for certification of private sector laboratories to perform evaluations to promote the testing of products and make available the results of such tests to agencies and to the public.

Committee views

The Committee affirms NIST's lead role in setting policy guidelines for computer security practices implemented by federal civilian agencies. The Committee encourages the greater use of commercially available security products by federal agencies by directing NIST to promote the use of such products whenever feasible and appropriate. In order to identify the most effective security products, the Committee tasks NIST to establish appropriate evaluation procedures and to establish requirements to certify the capability of private sector laboratories to conduct such tests.

The Committee expects NIST to expand its efforts to ensure the compliance of federal agencies with the information security and privacy guidelines developed by NIST in accordance with its statutory responsibilities. The Committee tasks NIST to develop metrics to assess the effectiveness of agencies' security and privacy programs, to conduct on-site evaluations of agencies' programs, and to report to Congress on the results of these evaluations.

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

Section 20 of the NIST Act is amended by 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 ($1,030,000 for FY 2001 and $1,060,000 for FY 2002) 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 and to publish reports and other information for public distribution.

Committee views

The Committee believes that an open and transparent system should be used by NIST in promulgating federal standards. The Computer System Security and Privacy Advisory Board (CSSPAB), acting as an independent board, is uniquely positioned to make recommendations to the Department of Commerce. This Board will be charged with submitting its recommendations along with NIST's proposals to the Secretary of Commerce for promulgation as regulations. The Board is being provided with resources and specific direction by the Committee to allow it to operate in an independent and autonomous fashion to pursue public policy issues that are important for assuring the security and integrity of computing and network systems, and the information they contain. The Board is authorized to convene public meetings and to publish reports and other information for public distribution.

The CSSPAB is to report directly to the Committee on Science of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate. The Committee emphasizes that CSSPAB reports do not require prior clearance by OMB or the Commerce Department before they are transmitted to the Congressional Committees.

Sec. 7. Limitation on participation in requiring encryption standards

Section 20 of the NIST Act is amended 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.

Committee views

NIST does not currently promulgate, enforce or otherwise adopt standards, or carry out activities or policies, for the federal establishment of encryption, or computer security standards required for use in computer systems other than Federal Government computer systems. It is the Committee's intention that NIST not be used for such purposes in the future.

Sec. 8. Miscellaneous amendments

Technical and conforming amendments to Section 20 of the NIST Act as well as a language change which reasserts NIST's role as

the lead agency for handling standards for civilian agency computer security.

Committee views

The Committee affirms NIST's role as the lead agency for handling standards for federal civilian agency computer security. The Committee believes that it is imperative that this function remain open to public scrutiny. NIST is the agency historically charged with setting the standards for computer security in the civilian agencies and it is the Committee's intention that NIST direct appropriate resources and expertise to this area.

Sec. 9. Federal computer system security training

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

Committee views

The Committee wishes to focus NIST's attention on security matters which have come about because of the changes in network information technology systems that have taken place since the enactment of the Computer Security Act of 1987. The World Wide Web is just one example of new developments in network technology programs which raise unique security concerns.

Sec. 10. Computer security fellowship program

Funds are authorized under Section 18 of the NIST Act to provide grants for research on computer security to students at institutions of higher learning ($500,000 for FY 2001 and $500,000 FY 2002).

Committee views

The Committee supports efforts to increase the number of college and graduate students in the field of computer security. NIST can play an important, although limited, role in this effort through its section 18 fellowship program.

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

This section authorizes funds ($450,000 for FY 2001 to remain available until expended) and sets terms for the National Research Council of the National Academy of Sciences to conduct a study of public key infrastructures (PKI) for use by individuals, businesses, and government.

Committee views

The Committee is aware that the Federal Government is aggressively promoting the deployment of PKI technology. PKIs are not yet commonplace in either the private sector or in government because a number of significant challenges must still be overcome before the technology can be widely deployed and implemented. The NRC study will provide valuable information on the costs, vulnerabilities and scalability issues of such an infrastructure.

Sec. 12. Promotion of national information security

Requires the Under Secretary of Commerce for Technology to actively promote the use of technologies that will enhance the security of 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 the standards-based infrastructure that will enable the more widespread use of encryption technologies for confidentiality and authentication.

Committee views

Through the requirements of section 12, the Committee intends to designate a central government focus for increasing public awareness of the need for improving the security of communications networks and the information accessed through such networks. The Committee notes that one of the central findings of the comprehensive 1996 report from the National Academy of Sciences, Cryptography's Role in Securing the Information Society, is the relative lack of attention paid to securing electronic information. Although the technical solutions for enhancing information security are available, the public has not been energized about the importance of utilizing these tools.

H.R. 2413 encourages greater use of commercially available cryptography products for protection of government information, which may have the indirect effect of enhancing the general availability of such technologies. To further increase public awareness of security threats and to accelerate corrective action, section 12 of the bill charges the Technology Administration in the Commerce Department to actively promote greater use of cryptography and associated technologies by the private sector. One specific requirement is for the Technology Administration to establish a clearinghouse of information for the public on information security threats to networked computers, including information about procedural and technical approaches to guard against such threats.

The Committee intends that the Technology Administration actively promote the development of a national, standards-based infrastructure to support the uses of encryption technologies for confidentiality and authentication by working closely with the private sector and by assisting and supporting the development of standards through a private-sector oriented, consensus-based process.

Sec. 13. Electronic authentication infrastructure

Directs NIST to work in consultation with industry to develop guidelines for electronic authentication infrastructures for use by federal agencies to ensure the security of transactions and interoperability with transaction partners. NIST will develop and maintain a list of conforming commercially available electronic authentication products used by federal agencies. NIST will develop criteria/guidelines for use by agencies for electronic management systems such as maintaining security of databases and validity of certificates. Eighteen months after enactment, NIST shall report to Congress on how agencies are deploying systems which are in accordance with guidelines developed by the agency. Guidelines developed by NIST or any Federal agency should be technology neutral.

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. The Technology Administration of the Department of Commerce shall appoint the National Panel and provide necessary administrative support.

Committee views

The Committee finds that digital signature technology is essential for the full use of public networks, such as the Internet, for commerce and for private communications. While P.L. 106–229, the Electronic Signatures in Global and National Commerce Act created the legal framework for the recognition and acceptance of electronic signatures, it does not address interoperability and other technical issues. Digital signatures verify the identity of a business or individual that is accessed via a network and assure the integrity of the information being exchanged. In order for digital signature technology to be deployed, in most cases, a trusted guarantor of the public identifier, or public key, of the digital signature must exist. This is the role of the certification authority.

The Committee is aware that several States have enacted statutes to regulate certification authorities. Unfortunately, this has largely been an uncoordinated process resulting in the placement of varying requirements on certification authorities. In order for a truly national system to develop, which is required if use of digital signatures is to become widespread, the Committee believes that uniform market driven consensus standards must be in place for the practices and procedures of the certification authorities. Otherwise, variations in the requirements for certification authorities will degrade the overall level of reliability and security of digital signatures.

To promote the required uniformity, section 13 of the bill establishes a national panel, under the auspices of the Technology Administration, to develop private voluntary model practices and procedures, promote uniformity among jurisdictions that license certification authorities, and private voluntary uniform audit standards for certification authorities. This national panel, with broadly based representation, including users of digital signature technology, will provide for the coordination needed to put in place the national technical infrastructure that is a prerequisite for the widespread use of digital signatures.

Sec. 14. Source of authorizations

This section authorizes $7 million in FY 2001 and $8 million in FY 2002 for NIST to carry out activities authorized by this Act for which funds are not otherwise specifically authorized.

Committee views

In addition to the funds authorized in H.R. 2413, H.R. 2086—the Networking and Information Technology Research and Development Act of 1999—which has passed the Science Committee and the House of Representatives—also authorizes funding for NIST to conduct fundamental computer security research in the area of advanced encryption standards and algorithms.

VIII. COST ESTIMATE

Rule XIII, clause 3(d)(2) of the House of Representatives requires each committee report accompanying each bill or joint resolution of a public character to contain: (1) an estimate, made by such committee, of the costs which would be incurred in carrying out such bill or joint resolution in the fiscal year in which it is reported, and in each of the five fiscal years following such fiscal year (or for the authorized duration of any program authorized by such bill or joint resolution, if less than five years); (2) a comparison of the estimate of costs described in subparagraph (1) of this paragraph made by such committee with an estimate of such costs made by any Government agency and submitted to such committee; and (3) when practicable, a comparison of the total estimated funding level for the relevant program (or programs) with the appropriate levels under current law. However, House rule XIII, clause 3(d)(3)(B) provides that this requirement does not apply when a cost estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974 has been timely submitted prior to the filing of the report and included in the report pursuant to House rule XIII, clause 3(c)(3). A cost estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974 has been timely submitted to the Committee on Science prior to the filing of this report and is included in this report pursuant to House rule XIII, clause 3(c)(3).

Rule XIII, clause 3(c)(2) of the House of Representatives requires each committee report that accompanies a measure providing new budget authority (other than continuing appropriations), new spending authority, or new credit authority, or changes in revenues or tax expenditures to contain a cost estimate, as required by section 308(a)(1) of the Congressional Budget Act of 1974 and, when practicable with respect to estimates of new budget authority, a comparison of the total estimated funding level for the relevant program (or programs) to the appropriate levels under current law. H.R. 2413 does not contain any new budget authority, credit authority, or changes in revenues or tax expenditures. Assuming that the sums authorized under the bill are appropriated, H.R. 2413 does authorize additional discretionary spending, as described in the Congressional Budget Office report on the bill.

IX. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, August 18, 2000.

Hon. F. JAMES SENSENBRENNER, Jr.
Chairman, Committee on Science,
House of Representatives, Washington, DC.

DEAR CONGRESSMAN: The Congressional Budget Office has prepared the enclosed estimate for H.R. 2413, the Computer Security Enhancement Act of 2000.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Taman Morris and Mark Hadley.

Sincerely,

ARLENE HOLEN
(For Dan L. Crippen, Director).

Enclosure.

H.R. 2413—Computer Security Enhancement Act of 2000

Summary: H.R. 2413 would direct the National Institute of Standards and Technology (NIST) to develop policies to improve computer security for federal computer systems and would authorize the appropriation of funds for this purpose in fiscal years 2001 and 2002.

CBO estimates that implementing the bill would cost $19 million over the 2001–2003 period, assuming appropriation of the authorized amounts. H.R. 2413 would not affect direct spending or receipts; therefore, pay-as-you-go procedures would not apply. The bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA).

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 2413 is shown in the following table. For this estimate, CBO assumes that H.R. 2413 would be enacted near the start of fiscal year 2001 and that the amounts authorized will be appropriated each year. Outlays have been projected on the basis of historical spending patterns for NIST and information provided by the agency. The cost of this legislation would fall within budget function 370 (commerce and housing credit).

	By fiscal year, in millions of dollars—				
	2001	2002	2003	2004	2005
CHANGES IN SPENDING SUBJECT TO APPROPRIATION					
Authorization level	9	10	0	0	0
Estimated outlays	7	10	2	0	0

Pay-as-you-go considerations: None.

Intergovernmental and private-sector impact: H.R. 2413 contains no intergovernmental or private-sector mandates as defined in UMRA. Any costs incurred by states to participate in the National Policy Panel for Digital Signatures are unlikely to be significant.

Estimate prepared by: Federal costs: Taman Morris and Mark Hadley; impact on State, local, and tribal governments: Victoria Heid Hall; impact on the private sector: Lauren Marks.

Estimate approved by: Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

X. COMPLIANCE WITH PUBLIC LAW 104–4

H.R. 2413 contains no unfunded mandates.

XI. COMMITTEE OVERSIGHT FINDINGS AND RECOMMENDATIONS

Rule XIII, clause 3(c)(1) of the House of Representatives requires each committee report to include oversight findings and recommendations required pursuant to clause 2(b)(1) of rule X. The

Committee on Science's oversight findings and recommendations are reflected in the body of this report.

XII. Oversight Findings and Recommendations by the Committee on Government Reform

Rule XIII, clause 3(c)(4) of the House of Representatives requires each committee report to contain a summary of the oversight findings and recommendations made by the House Government Reform Committee pursuant to clause 4(c)(2) of rule X, whenever such findings and recommendations have been submitted to the Committee in a timely fashion. The Committee on Science has received no such findings or recommendations from the Committee on Government Reform.

XIII. Constitutional Authority Statement

Rule XIII, clause 3(d)(1) of the House of Representatives requires each report of a committee on a bill or joint resolution of a public character to include a statement citing the specific powers granted to the Congress in the Constitution to enact the law proposed by the bill or joint resolution. Article I, section 8 of the Constitution of the United States grants Congress the authority to enact H.R. 2413.

XIV. Federal Advisory Committee Statement

H.R. 2413 does not establish nor authorize the establishment of any advisory committee

XV. Congressional Accountability Act

The Committee finds that H.R. 2413 does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act (Public Law 104–1).

XVI. Statement on Preemption of State, Local, or Tribal Law

The bill is not intended to preempt any state, local, or tribal law.

XVII. Changes in Existing Law Made by the Bill, as Reported

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

SECTION 20 OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT

Sec. 20. (a) * * *

(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) 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;

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

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

[(4)**]** *(8)* 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)**]** *(9)* 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) * * *

* * * * * * *

(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 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.

(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 2001 and $1,060,000 for fiscal year 2002 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**]** *may* draw upon computer system technical security guidelines developed by the National Security Agency to the

extent that the Institute 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;

* * * * * * *

(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.

SECTION 5 OF THE COMPUTER SECURITY ACT OF 1987

SEC. 5. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.

(a) * * *

(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[.]*; and*

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

* * * * * * *

XVIII. COMMITTEE RECOMMENDATIONS

On July 26, 2000 a quorum being present, the Committee on Science favorably reported H.R. 2413, Computer Security Enhancement Act of 2000, by a voice vote and recommends its enactment.

XIX. PROCEEDINGS OF THE SUBCOMMITTEE MARKUP

MARKUP ON H.R. 2413, THE COMPUTER SECURITY ENHANCEMENT ACT OF 1999

WEDNESDAY, OCTOBER 20, 1999

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE,
SUBCOMMITTEE ON TECHNOLOGY,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:37 a.m. in room 2318, Rayburn House Office Building, Hon. Constance A. Morella (chairwoman of the subcommittee) presiding.

Chairwoman MORELLA. I am going to convene the Technology Subcommittee of the Science Committee. Good morning. Pursuant to notice, the Subcommittee on Technology is meeting today. We are going to consider H.R. 2413, 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.

I ask unanimous consent for the authority to recess at any point. Hearing no objection, so ordered.

Today we have one item of business to bring before the Subcommittee; that is, the bill H.R. 2413, a bill to enhance the ability of the National Institute of Standards and Technology to improve computer security.

Computer security, as we all know, is an issue that is a priority not just with the Technology Subcommittee, but also by the Science Committee. In just this year, the Subcommittee has held three hearings on this important issue, that has the potential to disrupt public and private sector businesses, as well as to undermine the American people's confidence and trust in our rapidly developing information technology systems.

In April, this Subcommittee met to explore the impact of the Melissa computer virus and other evolving threats to computer and information security. In June, in the face of several well-publicized cyberattacks, we met to review the security of federal agency websites. And last month, we met to review the provisions of H.R. 2413, the legislation that we are marking up today.

In our hearings we repeatedly heard that federal agencies are not doing enough to protect their critical information systems from attacks and corruption. The Federal Government is not alone in its need to secure electronic information; the corruption of electronic data threatens every sector of our economy.

H.R. 2413 was introduced in July by myself, Chairman Sensenbrenner of Wisconsin, and Congressman Gordon of Tennessee. It strengthens the National Institute of Standards and Technology's historic role in computer security, which was established by the Computer Security Act of 1987.

What the bill does is update the decade-old act, while giving NIST the tools it needs to ensure that appropriate attention and effort is concentrated on securing our federal information technology infrastructure.

I don't think it is necessary to go through each of the details of the bill. I will, if unanimously approved, just simply submit it all for the record. Hearing no objection, so ordered.

[A copy of H.R. 2413 follows:]

I

106TH CONGRESS
1ST SESSION

H. R. 2413

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

JULY 1, 1999

Mr. SENSENBRENNER (for himself, Mr. GORDON, and Mrs. MORELLA) 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 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 re-

sponse 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 thereafter, 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 sig-

nature 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 effectively 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.

○

Chairwoman MORELLA. It is a very important bill, as we all know. Last Congress, both the House of Representatives and the Senate Commerce Committee passed this same legislation without opposition or amendment, and unfortunately the bill didn't clear the Senate before the end of the 105th Congress.

While no single piece of legislation can fully protect our federal civilian computer systems or overcome all barriers to the creation of an interoperable electronic signature infrastructure, I think that H.R. 2413 is an important step in the right direction, so I urge all members to support its swift passage today, to move the bill on to the full Science Committee.

I am now pleased to recognize Mr. Barcia, the distinguished ranking member of the Subcommittee, for any opening statement he may have.

Mr. BARCIA. Thank you very much, Chairwoman Morella. I will be very brief in my remarks on H.R. 2413.

When the Subcommittee held a hearing on this bill on September 30th, I raised my concerns about the lack of a strong focal point to advise agencies on improving computer security practices and ensuring that such practices are implemented. H.R. 2413 strengthens the role of NIST in providing federal agencies with these services. The provisions of H.R. 2413 are entirely consistent with recommendations made by NIST's Private Sector Advisory Board and the witnesses at our recent hearing.

In addition, the inclusions of Mr. Gordon's provisions on electronic authentication technologies improves the security of federal agencies' electronic transactions. More importantly, these provisions provide a framework that will enable federal agencies to begin to effectively implement the Government Paperwork Elimination Act, which requires them to begin using electronic authentication technologies.

I would also request that Chairwoman Morella continue to work with us to clarify Section 7 of this bill. This language is unduly broad and could be interpreted to prevent NIST from working with industry to develop test beds and guidelines related to electronic commerce and computer security. For example, the language as drafted could be interpreted to prevent NIST from developing the follow-on to the Digital Encryption Standard, or DES. The current Digital Encryption Standard is widely used in industry, and NIST's work in this area has strong industry support.

No one on this Committee supports the concept of federal standards that industry must follow, and neither does NIST. Although the concept behind this section is well-intentioned, as drafted it would limit NIST's activities to support industry's development of electronic commerce and computer security. H.R. 2413 would strengthen the overall security of federal computer systems and their electronic transactions.

This bill establishes a blueprint for the Federal Government to become a model for good computer security practices. I fully support this legislation and urge my colleagues to support this well-crafted bill.

I want to thank you, Chairwoman Morella, and with your indulgence I would like to yield the balance of my time to the distinguished Member from Tennessee, who has invested a great deal of his time and energy into crafting this legislation and enhancing

and improving the language in it, Representative Bart Gordon of Tennessee.

Chairwoman MORELLA. The distinguished Member from Tennessee is recognized.

Mr. GORDON. Thank you, Mr. Barcia, for the good job you have done, and Chairwoman Morella, on this bill, and thank you for yielding to me. I also want to thank the staff for all the work they have put into this bill.

I know most of you are sitting on the edge of your seats, waiting for this electronic authentication technology bill to pass. But for the ones of you who may not have been following it, let me give you a quick update.

Some years ago we passed the Government Paperwork Elimination Act. That is going to allow us to reduce a lot of paperwork within the government so that agencies can communicate with each other, up and down and across, electronically. However, we neglected to set any kind of—I hate to use the word "standards"—but ability for them to do so in a way that there is continuity. It doesn't help if Department of Agriculture at different levels have different types of authentication so that they can't communicate with each other. And so what this will do, it would allow NIST to set up a framework, just simply guidelines, so that the agencies will know that particular types of—hopefully—software, off the shelf, will allow them to communicate with their own agencies as well as others, and also allow them to set up an appropriate level of security. Obviously, routine work takes less security needs than other things.

So I think it will help us to really, truly eliminate paperwork and allow some continuity, and I thank you for working with me on this provision.

Chairwoman MORELLA. I thank you, Mr. Gordon, for your contribution to this bill.

[The statement of Hon. Debbie Stabenow follows:]

SUBCOMMITTEE ON TECHNOLOGY

MARKUP OF H.R. 2413, THE COMPUTER SECURITY ENHANCEMENT ACT OF 1999

Opening Statement of Congresswoman Debbie Stabenow
of the 8th District, State of Michigan

October 20, 1999

Madame Chairwoman, Ranking Member Barcia, I am pleased the Subcommittee is proceeding this morning with the markup of this important legislation. As we heard at a hearing just a few weeks ago, this bill is an important step toward refocusing efforts to ensure the security of federal computer systems. As I said at the last hearing, the Internet, e-mail, and the speed of computers have added a new dynamic to the threat of computer hacking and terrorism. The fact the Department of Defense endured 250,000 hacker attempts last year alone is indicative of this trend. The threat of cyber-attack makes it imperative that federal computer security efforts are updated and robust.

Madame Chairwoman, I appreciate the leadership that the Subcommittee leadership on both sides of the aisle have shown on these important issues, and I would also like to acknowledge the work that Mr. Gordon has done on digital signatures. His legislation is an important addition to H.R. 2314, and I look forward to moving this legislation on to the full Committee and hopefully soon to the House floor.

I don't think anyone else has any opening statements, so we will move as quickly as possible.

As we now consider H.R. 2413, I ask unanimous consent that the bill be considered as read and open to amendment at any point, and I ask members to proceed with the amendments in the order on the roster. And therefore, in our desire to move ahead, I am going to offer an amendment, a Manager's Amendment, a bipartisan Manager's Amendment, crafted in careful consideration with the Ranking Member Barcia.

The Clerk will report the amendment.

The CLERK. Amendment to H.R. 2413, offered by Mrs. Morella and Mr. Barcia——

Chairwoman MORELLA. I ask unanimous consent to dispense with the reading.

I recognize myself for five minutes, but I will take less time than that to explain the amendment.

In cooperation with the Ranking Member Barcia, I am pleased to offer the bipartisan amendment that has been crafted to improve the bill. According to the General Accounting Office and other computer security experts, there is a dire need for agencies to realize their computer security vulnerabilities and to take immediate action to address them.

The amendment tasks NIST to utilize their computer security expertise to assess existing information security programs of federal agencies, and then to make recommendations to improve their security. What NIST would do is report to Congress annually on the information security status of our federal agencies. We found this to be very, very important.

NIST would also document on the process and progress of agencies to implement recorded and recommended security improvements.

[The amendment offered by Mrs. Morella and Mr. Barcia follows:]

AMENDMENT TO H.R. 2413

OFFERED BY MRS. MORELLA AND MR. BARCIA

Page 3, line 6, strike "(7), and (8)" and insert "(8), and (9)".

Page 3, line 24, through page 4, line 9, strike paragraphs (5) and (6) and insert the following:

"(5) to provide guidance and assistance to Federal agencies in the protection of information security in interconnected Federal computer systems, including identification of significant risks thereto;

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

"(7) to coordinate Federal response efforts related to unauthorized access to Federal computer systems;".

Page 4, line 17, insert "(1)" after "(c)".

Page 4, lines 19 and 22, and page 5, line 1, redesignate paragraphs (1) through (3) as subparagraphs (A) through (C), respectively.

Page 5, after line 7, insert the following:

"(2) In carrying out subsection (a), the Institute shall perform evaluations and tests—

"(A) at Federal agencies to assess existing information security and privacy programs; and

"(B) of commercially available security products for their conformance with guidelines and standards developed under subsection (a)(2) and (3).

"(3) The Institute shall maintain and make available to Federal agencies and to the public a list of commercially available security products evaluated under paragraph (2)(B) as conforming with the guidelines and standards developed under subsection (a)(2) and (3).

"(4) The Institute shall annually transmit to the Congress 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 evaluated under paragraph (2)(B);

"(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 de-

scribed in subparagraph (A), and the response by the agencies to those recommendations.".

Page 5, lines 19 through 22, strike "No standards" and all that follows through "written recommendations.".

Chairwoman MORELLA. The rest of my statement I am going to submit for the record, but frankly, it enhances the role of NIST in protecting the information security of federal agencies.

[The statement of Mrs. Morella follows:]

Chairwoman Constance A. Morella
Subcommittee Mark-up of H.R. 2413
Morella/Barcia En Bloc Amendment

October 20, 1999

In cooperation with Ranking Member Barcia, I am pleased to offer this bipartisan amendment that has been crafted to improve H.R. 2413, as introduced.

According to the General Accounting Office and other computer security experts, there is a dire need for agencies to realize their computer security vulnerabilities and to take immediate steps to address them.

This amendment tasks NIST to utilize their computer security expertise to assess existing information security programs of Federal agencies and then to make recommendations to improve their security.

NIST would report to Congress annually on the information security status of our federal agencies.

NIST would also document on the progress of agencies to implement recommended security improvements.

The addition of these important provisions gives this Committee the tools we need to provide responsible oversight on the critical issue of Federal agencies and their efforts to improve information security – much like we have done with our oversight of federal agencies and the Year 2000 computer problem.

While this amendment enhances the role of NIST in protecting the information security of Federal agencies, it does not shift the responsibility away from the agencies. Ultimately, agencies bear the primary responsibility for maintaining the security of their information systems.

Finally, the amendment makes certain changes to Section 6 of the bill as recommend by the Computer System Security and Privacy Advisory Board and NIST.

I urge all members to support this bipartisan amendment.

Chairwoman MORELLA. It doesn't shift any responsibility away from the agencies, but will also allow for some oversight.

Finally, the amendment makes certain changes to Section 6 of the bill, as recommended by the Computer Systems Security and Privacy Advisory Board and NIST. I urge all members to support this bipartisan amendment.

At this point I want to recognize the Ranking Member of the Subcommittee, Mr. Barcia, to speak on behalf of the amendment.

Before we do that, I want to note the presence of a recording quorum.

Mr. Barcia.

Mr. BARCIA. I want to thank Chairwoman Morella for her thorough but concise explanation of the en bloc amendment. I, too, have a more lengthy statement to make in support of the en bloc amendment, and I certainly would urge my colleagues to support the amendment.

I would just like to, on the record, though, however, say that I do have one small reservation. This amendment increases NIST's responsibilities to assist agencies in protecting their information systems without providing any additional funding to carry out these additional responsibilities. Discussions with the General Accounting Office indicate that security checks of civilian agencies' information systems would cost around $4.8 million per year. If this Committee is serious about strengthening this role in this area, we must provide the resources to enable them to carry out the responsibilities. The issue of inadequate resources has been the major concern of NIST's Advisory Board from its beginning.

I would hope that Chairwoman Morella would work with us in a bipartisan way, as she has in the past, to help resolve this issue before we proceed to the full Committee level.

With those brief remarks, I want to say I fully support the en bloc amendment, and in the interest of time will not touch on the strong recommendations I have in terms of the other language that has been worked out. I just wanted to go on the record with that one reservation I have about the resources being there to carry out the responsibilities we're assigning.

[The statement of Mr. Barcia follows:]

Statement

Hon. James A. Barcia (D-MI)

Morella/Barcia En Bloc Amendment

H.R. 2413, The Computer Security Enhancement Act of 1999

20 October 1999

Chairwoman Morella has outlined the provisions in the amendment, so I will not go through the specific provisions again. I would just like to highlight that this amendment is the result of recommendations made by the Computer System Security and Privacy Board, the General Accounting Office and the National Security Agency.

In 1997, the Advisory Board sent the Technology Subcommittee a statement by its chairman about the need to strengthen the implementation of the Computer Security Act. The Board recommended reinforcing the commitment of NIST to provide direct assistance to civilian agencies on their information system security needs. In fact, the Advisory Board passed Resolution 97-1 in June 1997 that calls on NIST to provide a central service in the federal government to advise agencies on the selection, integration, and use of products and procedures for securing non-classified systems as well as to provide a computer systems security assessment capability for civilian agencies. Last month, during the Subcommittee's hearing on H.R. 2413, GAO testified about the urgent need to strengthen computer security across the federal government on the basis of its past audits. GAO stressed that there was no mechanism to routinely test and evaluate the effectiveness of agencies' information security programs.

In addition, the Computer System Security and Privacy Advisory Board's Resolution 97-1 called on NIST to maintain a repository and act as a clearinghouse for information, techniques, guidelines, and consultation to aid proper use of security features available in government-used commercial off-the-shelf software. When the National Security Administration (NSA) appeared before the Technology Subcommittee in June of this year, the NSA witness pointed out that exaggerated claims are sometimes made about the security functionality of commercial products. He recommended that federal agencies need a list of independently evaluated products for procurement purposes. The NSA witness also suggested that products that have undergone stringent evaluation and have been found to be satisfactory for security purposes should be agencies' first choice.

This en bloc amendment, which I have drafted with Chairwoman Morella, specifically addresses these concerns. I would urge my colleagues to support this amendment.

Chairwoman MORELLA. Thank you, Mr. Barcia. I think everybody knows that NIST is located in my District, and I, along with this Committee, have been a strong advocate for it. As H.R. 2413 moves forward to the full Science Committee for consideration, I intend to work with our Ranking Member and with Chairman Sensenbrenner to identify additional funding for NIST to carry out the important responsibilities required under the bill. I think it is a very important point that you bring up.

I wonder if there is any discussion on the amendment?

[No response.]

Chairwoman MORELLA. If no, the vote occurs on the amendment. All in favor, say aye.

[Chorus of ayes.]

Chairwoman MORELLA. Opposed, no.

[No response.]

Chairwoman MORELLA. The yeas have it. The amendment is agreed to.

Any further amendments?

[No response.]

Chairwoman MORELLA. Hearing none, the question is on the bill, H.R. 2413, as amended. All those in favor will say aye.

[Chorus of ayes.]

Chairwoman MORELLA. All those opposed will say no.

[No response.]

Chairwoman MORELLA. In the opinion of the Chair the ayes have it.

Mr. Barcia.

Mr. BARCIA. Yes, Madam Chairwoman. I move that the Subcommittee favorably report H.R. 2413, as amended, to the full Committee, and that the Chairwoman take all such necessary steps to bring the bill before the full Committee for consideration.

Further, I ask unanimous consent that the staff be instructed to make all necessary technical and conforming changes to the bill.

Chairwoman MORELLA. The Subcommittee has heard the motion. Those in favor will say aye.

[Chorus of ayes.]

Chairwoman MORELLA. Those opposed, no.

[No response.]

Chairwoman MORELLA. The ayes have it. The motion is agreed to. Without objection, the motion to reconsider is laid upon the table.

I move that members have two subsequent calendar days in which to submit supplemental, minority, or additional views on the measure. Without objection, the motion is adopted.

Mr. Barcia had raised section 7. It was pointed out to me that—I wanted to just have the record show that section 7 is necessary because there is a great deal of concern by the private sector that the Federal Government is interested in setting standards that would be forced upon the private sector. And it wasn't long ago when NIST and the National Security Agency were involved in the Federal Government's so-called "Clipper Chip" initiative, and in that case the Federal Government attempted to set a standard in a manner that gave them the keys to otherwise private information.

So I am going to include further response to your question of section 7 for the record.

[Information to be supplied follows:]

Chairwoman Constance A. Morella
Subcommittee Mark-up of H.R. 2413
Comments on Section 7 of H.R. 2413.

Section 7 of H.R. 2413 is necessary because there is a lot of concern from industry and privacy advocates that the Federal government is interested in setting standards that will be forced upon the private sector. It was not that long ago that NIST and the National Security Agency were involved in the Federal government's "Clipper Chip" initiative. In that case, the Federal government attempted to set a standard in a manner that gave them the "keys" to otherwise private information. Industry and the privacy advocates still harbor significant levels of mistrust towards the Federal government regarding any efforts to set standards under the guise of security.

Section 7 is intended to foster a more collaborative, cooperative relationship between industry and the Federal government where ideas and information can be shared in an open, trustworthy environment. Section 7 will not in any way prevent NIST from promulgating computer security guidelines or recommendations. Nor is this provision intended to prevent NIST from working with industry on the new Advanced Encryption Standard due out next year. I would be happy to work with my colleague to draft appropriate Committee Report language to clarify this provision in a manner that satisfies his concerns that would be offered during full-committee consideration of H.R. 2413.

Chairwoman MORELLA. That being the case, the bill is approved by this Subcommittee in a very expeditious and wise fashion, and it will be reported to the full Committee, and staff have the authority to do what has to be done to bring it to the full Committee for its deliberate and expeditious passage.

I thank the Subcommittee. You have been just great. There is now a vote on the Journal, and the Subcommittee is now adjourned.

[Whereupon, at 10:51 a.m., the Subcommittee was adjourned, to reconvene at the call of the Chair.]

XX. PROCEEDINGS OF THE FULL COMMITTEE MARKUP

BUSINESS MEETING

WEDNESDAY, JULY 26, 2000

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE,
Washington, DC.

The committee met, pursuant to call, at 2:04 p.m. in room 2318, Rayburn House Office Building, Hon. F. James Sensenbrenner, Jr. (chairman of the committee) presiding.

Chairman SENSENBRENNER. We will now go back to H.R. 2413, the Computer Security Enhancement Act of 1999, as amended by the Subcommittee on Technology.

This bill has been introduced by myself, Mr. Gordon, Mrs. Morella, and Mr. Kuykendall. The legislation strengthens the National Institute of Standards and Technology's historical role in computer security that was established by the Computer Security Act of 1987, Public Law 100-235, and updates the act to give NIST the tools it needs to ensure that appropriate attention and effort is concentrated on securing our Federal information technology infrastructure.

Let me point out that this bill is not a knee-jerk reaction to recent well-publicized computer security problems. In the last Congress, this bill passed the House and was cleared by a Senate Committee without opposition or amendment but was unable to reach the Senate Floor before the 105th Congress adjourned. Improving the information security of Federal civilian agencies has been an oversight priority of the Science Committee and I am now pleased that H.R. 2413 will play an important role in this effort.

[A copy of the bill H.R. 2413 follows:]

[COMMITTEE PRINT]

(Showing H.R. 2413 as amended by the Subcommittee on Technology on October 20, 1999)

106TH CONGRESS
1ST SESSION

H. R. 2413

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

JULY 1, 1999

Mr. SENSENBRENNER (for himself, Mr. GORDON, and Mrs. MORELLA) 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 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 secu-

rity 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), (8), and (9), 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 information security in interconnected Federal computer systems, including identification of significant risks thereto;

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

"(7) to coordinate Federal response efforts related to unauthorized access to Federal 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)(1) In carrying out subsection (a)(3), the Institute shall—

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

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

"(C) 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.

"(2) In carrying out subsection (a), the Institute shall perform evaluations and tests—

"(A) at Federal agencies to assess existing information security and privacy programs; and

"(B) of commercially available security products for their conformance with guidelines and standards developed under subsection (a)(2) and (3).

"(3) The Institute shall maintain and make available to Federal agencies and to the public a list of commercially available security products evaluated under paragraph (2)(B) as conforming with the guidelines and standards developed under subsection (a)(2) and (3).

"(4) The Institute shall annually transmit to the Congress 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 evaluated under paragraph (2)(B);

"(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. 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). 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 (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. 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 dissemina-

tion 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 thereafter, 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 Sec-

retary 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 effectively 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.

Chairman SENSENBRENNER. I will now recognize the gentleman from Texas, Mr. Hall, for his opening statement on this bill. The gentleman is recognized for five minutes.

Mr. HALL. Thank you, Mr. Chairman. Before I yield to Mr. Gordon, I would like to compliment him, Mrs. Morella, and others for their very hard work on the question of computer security. This has been a very important topic for the Committee for about 15 years, and dating back to when this Committee worked with Congressman Jack Brooks to enact the first computer security law dealing with federally owned computers.

H.R. 2413 brings our computer security efforts into the Internet age by working to upgrade security of Federal computer systems and networks. Thanks to the ideas of Mr. Gordon and to others, it will also permit the Federal Government to advance e-commerce and e-government by providing for secure electronic authentication technology.

I plan to support the Morella-Gordon amendment in the nature of a substitute and I urge my colleagues to do so.

I yield the balance of my time to Congressman Bart Gordon. And before Mr. Gordon reports, I will yield to Mr. Barcia.

[The prepared statement of Mr. Hall follows:]

STATEMENT OF HON. RALPH M. HALL

Mr. Chairman, before, I yield to Mr. Barcia, the Technology Subcommittee Ranking Member, I would like to complement him, Mrs. Morella, and Mr. Gordon for their hard work on the question of computer security. This has been an important topic for the Committee for 15 years or more, dating to when this Committee worked with Congressman Jack Brooks to enact the first computer security law dealing with Federally-owned computers.

H.R. 2413 brings our computer security efforts into the Internet age by working to upgrade security of Federal computer systems and networks. Thanks to the ideas of Mr. Gordon, it also will permit the Federal government to advance e-Commerce and e-Government by providing for secure electronic authentication technologies.

I plan to support the Morella-Gordon amendment in the nature of a substitute and urge my colleagues to do so as well.

I yield the balance of my time to Congressman Barcia.

Mr. BARCIA. Thank you very much, Ranking Member Hall.

Mr. Chairman, I will be very brief. H.R. 2413, the Computer Security Enhancement Act, represents more than four years of effort by the Technology Subcommittee. During the past two years, the Subcommittee has examined the impact of computer viruses and the lack of good computer security practices at Federal agencies. H.R. 2413 strengthens the role of NIST in providing Federal agencies with needed advice on good security practices.

The provisions of H.R. 2413 are entirely consistent with recommendations made by NIST's private sector advisory board and the witnesses who testified at our hearings. The inclusion of Mr. Gordon's provisions on electronic authentication technologies also serves to improve the security of Federal agencies' electronic transactions. In addition, the provisions provide a framework to enable Federal agencies to effectively implement the Government Paperwork Elimination Act, which requires agencies to begin using electronic authentication technologies.

H.R. 2413 will strengthen the overall security of Federal computer systems and their electronic transactions. This bill establishes a blueprint for the Federal Government to become a model

for good computer security and authentication practices. The Technology Subcommittee reported this bill with unanimous support.

I also want to say that I support the amendment in the nature of a substitute to be offered by Representatives Gordon and Morella, and I would urge all of my colleagues to support this bill. And once again I thank the Chair of the Subcommittee for all of her diligent work on this issue and the hearings that were held as well as Congressman Gordon. And I yield my time back.

Chairman SENSENBRENNER. You have got two minutes left.

Mr. HALL. I yield back my time, sir.

Chairman SENSENBRENNER. Okay. Time is yielded back.

Without objection, other members may insert opening statements at this point in the record.

The Chair is aware of only one amendment in the nature of a substitute by Mrs. Morella and Mr. Gordon. And at this point, the Chair recognizes the gentlewoman from Maryland.

Mrs. MORELLA. Thank you, Mr. Chairman. And I do have an amendment at the desk.

Chairman SENSENBRENNER. The Clerk will report the amendment.

The CLERK. Amendment in the nature of a substitute to H.R. 2413, offered by Mrs. Morella and Mr. Gordon.

Mrs. MORELLA. Mr. Chairman, I move that the amendment be considered as read.

Chairman SENSENBRENNER. Without objection. And the gentlewoman is recognized for five minutes.

Mrs. MORELLA. Thank you. I am pleased to offer this bipartisan amendment to improve H.R. 2413. It has been crafted in cooperation with Congressman Bart Gordon.

First of all, Mr. Chairman, I want to thank you and Mr. Hall for bringing this bill up. I want to thank Mr. Barcia for continuing the legacy that began with Mr. Gordon and myself. This bill, as you mentioned, has passed in the previous Congress and here it is back again, a new enhanced version which we hope will get through the House and through the Senate.

Over the past two years, the Technology Subcommittee, we have had a series of computer security hearings, including a specific legislative hearing focusing on this bill. As amended, H.R. 2413 authorizes $9 million in fiscal year 2001, and $9.5 million in fiscal year 2002 for the National Institute of Standards and Technology. What these funds would do is they would allow NIST to promote the use of commercially available off-the-shelf security products by Federal agencies, have an independent advisory board review NIST's computer security and privacy protection efforts and make recommendations, create a fellowship program in the field of computer security to address IT worker shortages, establish an expert review team to assist agencies to identify and fix existing information security vulnerabilities.

Mr. Chairman, while no single piece of legislation can fully protect our Federal civilian computer systems, we really feel that H.R. 2413 is a necessary step in the right direction. It has already been favorably reported by the Technology Subcommittee, endorsed by the Information Technology Association of America, and I strongly urge all members to support this amendment and this important legislation.

You know, we took care of the Y2K computer glitch but that had a terminal period of January 1st and February 29th of this year. But computer security goes beyond, and it is international in scope, and this legislation is a good step toward trying to remediate that terrible problem. And I yield back, Mr. Chairman.

[The statement on the amendment in the nature of a substitute offered by Mrs. Morella follows:]

I am pleased to offer this bipartisan amendment to improve H.R. 2413 that has been crafted in cooperation with Congressman Bart Gordon.

Over the past two years, the Technology Subcommittee has held a series of computer security hearings, including a specific legislative hearing focusing on the bill.

As amended, H.R. 2413 authorizes $9 million in FY 2001 and $9.5 million in FY 2002 for the National Institute of Standards and Technology.

The funds would allow NIST to:

Promote the use of commercially available off-the-shelf security products by federal agencies, an initiative strongly supported by the Information Technology Association of America and others;

Increase privacy protection by giving an independent advisory boards more responsibility and resources to review NIST's computer security efforts and to make recommendations;

Support the development of a well trained workforce by creating a fellowship program in the field of computer security;

Study the efforts of the Federal government to develop a secure, interoperable electronic infrastructure; and finally,

Establish an expert review team to assist agencies to identify and fix existing information security vulnerabilities.

The General Accounting Office and other computer security experts have all recognized the need for H.R. 2413.

Mr. Chairman, while no single piece of legislation can fully protect our federal civilian computer systems; H.R. 2413 is a necessary step in the right direction.

It has already been favorably reported by the Technology Subcommittee and I strongly urge all members to support this amendment to this important legislation.

Thank you.

COMMITTEE ON SCIENCE FULL COMMITTEE MARKUP, JULY 26, 2000—AMENDMENT ROSTER FOR H.R. 2413, COMPUTER SECURITY ENHANCEMENT ACT OF 1999

No. and sponsor, description, results:

1. Mrs. Morella and Mr. Gordon, amendment to H.R. 2413, adopted by a voice vote.

AMENDMENT IN THE NATURE OF A SUBSTITUTE H.R. 2413 OFFERED BY MRS. MORELLA AND MR. GORDON

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Security Enhancement Act of 2000".

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. 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), (8), and (9), 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) 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;

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

"(7) in consultation with appropriate Federal agencies, assist Federal response efforts related to unauthorized access to Federal 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)(1) In carrying out subsection (a)(2) and (3), the Institute shall—

"(A) emphasize the development of technology-neutral policy guidelines for computer security 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. 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). 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 2001 and $1,060,000 for fiscal year 2002 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 (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. 10. COMPUTER SECURITY FELLOWSHIP PROGRAM.

There are authorized to be appropriated to the Secretary of Commerce $500,000 for fiscal year 2001 and $500,000 for fiscal year 2002 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 2001, 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 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) promote the development of the national, standards-based infrastructure needed to support government, 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 18 months after the date of the enactment of this Act, the Director, in consultation with industry and appropriate Federal agencies, shall develop electronic authentication infrastructure guidelines and standards for use by Federal agencies to assist those agencies to 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 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 consultation with the National Policy Panel for Digital Signatures established under subsection (e).
(4) REVISIONS.—The Director shall periodically review the guidelines and standards developed under paragraph (1) and revise them as appropriate.

(b) LISTING OF VALIDATED 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 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) 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) an evaluation of the extent to which Federal agencies' electronic authentication infrastructures conform to the guidelines and standards developed under subsection (a)(1).

(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 effectively utilize electronic authentication technologies;

(7) the term "electronic certification and management technologies" 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 $7,000,000 for fiscal year 2001 and $8,000,000 for fiscal year 2002, 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.

Chairman SENSENBRENNER. The gentlewoman yields back the balance of her time.

Is there further discussion on the amendment?

The gentleman from Tennessee.

Mr. GORDON. Mr. Chairman, I move to strike the last word.

Chairman SENSENBRENNER. The gentleman is recognized for five minutes.

Mr. GORDON. Thank you. First, I want to thank Chair Morella for working in such a bipartisan manner on this amendment. Primarily, the amendment incorporates comments and clarifications that we received from the Administration on the electronic authentication provisions in the bill. However, we also have strengthened this role in improving security practices at Federal agencies as well as advising them on the effective deployment of electronic authentication technologies.

The underlying principle of H.R. 2413 and this amendment is that they recognize that government and the private sector computer security needs are similar. This amendment ensures that the private sector has a strong voice in the development of any electronic authentication guidelines for use by Federal agencies and that the agencies rely on commercially available products and services as much as possible.

I also want to thank Chairman Sensenbrenner for his leadership on this issue and for working closely with me on the development of this legislation. We both have been motivated by the importance that we place on the Science Committee to act on the broad issue of electronic security. Additionally, I want to thank Mike Quear for the long and good hours of staff work on this issue. This has been a good bill, is a good amendment, and it represents sound policy. I urge my colleagues to support this amendment.

[The prepared statement of Mr. Gordon follows:]

STATEMENT OF HON. BART GORDON

Mr. Chairman, First, I want to thank Chair Morella for working in such a bipartisan manner on this amendment.

Primarily, the amendment incorporates comments and clarifications that we received from the Administration on the electronic authentication provisions in the bill.

However, we have also strengthened NIST's role in improving computer security practices at federal agencies as well as advising them on the effective deployment of electronic authentication technologies.

The underlying principle of H.R. 2413 and this amendment is that they recognize that government and private sector computer security needs are similar.

This amendment ensures that the private sector has a strong voice in the development of any electronic authentication guidelines for use by federal agencies and that agencies rely on commercially available products and services as much as possible.

I also want to thank chairman Sensenbrenner for his leadership on this issue and for working closely with me on the development of this legislation.

We have both been motivated by the importance that we place on the Science Committee to act on the broad issue of electronic security.

This is a good bill, a good amendment and it represents sound policy. I would urge my colleagues to support this amendment.

Chairman SENSENBRENNER. Does the gentleman yield back?

Mr. GORDON. Yes.

Chairman SENSENBRENNER. Further discussion on the amendment?

Ms. LOFGREN. Mr. Chairman.

Chairman SENSENBRENNER. The gentlewoman from California.

Ms. LOFGREN. I move to strike the last word.

Chairman SENSENBRENNER. The gentlewoman is recognized for five minutes.

Ms. LOFGREN. Mr. Chairman, I would like to thank members on both sides of the aisle for working to address some concerns that this bill in its original form raised for me. I think that this amendment in the nature of a substitute offered by Mr. Gordon and Mrs. Morella is a real step in the right direction and I am very happy to support it.

I look forward to continuing to work with members on the Committee Report to this bill to clarify that our intentions are unanimously benign relative to encryption and key recovery. In particular, I hope that the report will emphasize that we are in no manner encouraging the promulgation of third party encryption key recovery systems into the private sector. In addition, I hope it will express that we do not intend, the Federal Government, through the force of its purchasing powers, one of the world's largest contractors, to impose its encryption standards and regulations on the companies with which it does business.

I look forward to working further with my colleagues and I greatly appreciate their tremendous and well-guided efforts on this bill to this point, and in particular this bipartisan amendment. And I yield back.

[The prepared statement of Ms. Lofgren follows:]

STATEMENT OF HON. ZOE LOFGREN

Mr. Chairman, I would like to thank Members on both sides of the aisle for working to address some concerns that this bill in its original form raised for me. I think that this amendment in the nature of a substitute offered by Mr. Gordon and Mrs. Morella is a real step in the right direction, and I am very happy to support it. I look forward to continuing to work with Members on the Committee Report to this bill to clarify that our intentions are unanimously benign relative to encryption technology.

In particular, I hope that the Report will emphasize that we are in no manner encouraging the promulgation of third-party encryption key recovery systems into the private sector. In addition, I hope it will express that we do not intend the Federal Government, through the force of its purchasing powers as one of the world's largest contractors, to impose its encryption standards and regulations on companies with which it does business. I look forward to working further with my colleagues and I greatly appreciate their tremendous and well-guided efforts on this bill to this point and, in particular, this bipartisan amendment.

Chairman SENSENBRENNER. Will the gentlewoman yield?

Ms. LOFGREN. I certainly will, sir.

Chairman SENSENBRENNER. The Chair enthusiastically endorses the request of the gentlewoman from California to put the language in the Report language so that we can make it quite clear that this is a cooperative venture rather than a hammer in the hand of the Federal Government.

Ms. LOFGREN. Thank you, Mr. Chairman. I yield back.

Mrs. MORELLA. Mr. Chairman.

Chairman SENSENBRENNER. The gentlewoman from Maryland has already been recognized on this amendment. Somebody else want to move to strike the last word?

Mr. ETHERIDGE. I move to strike the last word.

Chairman SENSENBRENNER. The gentleman from North Carolina is recognized for five minutes.

Mr. ETHERIDGE. I yield to the lady from Maryland.

Mrs. MORELLA. I thank the gentleman for yielding. And I really only need probably about 30 seconds simply to indicate that I do understand the concerns that the gentlewoman from California posed with regard to Section 7. I just want to reiterate that it was really intended to be a safeguard to reflect the concerns, what she was offering, the concerns of the private sector and to reiterate the fact that it is not intended to prevent NIST from working with industry to develop voluntary—voluntary encryption standards and guidelines. So I emphasize on a voluntary basis. I yield back. I thank the gentleman from North Carolina.

Chairman SENSENBRENNER. Further discussion on the amendment?

[No response.]

Chairman SENSENBRENNER. Hearing none, all those in favor of the amendment in the nature of a substitute by Mrs. Morella and Mr. Gordon will signify by saying aye.

[Chorus of ayes.]

Chairman SENSENBRENNER. Opposed, no.

[No response.]

Chairman SENSENBRENNER. The ayes have it, and the amendment is agreed to.

Are there further amendments to the bill?

[No response.]

Chairman SENSENBRENNER. Hearing none, the Chair recognizes the gentleman from Michigan for purposes of a motion.

Mr. BARCIA. Thank you, Mr. Chairman. I move that the Committee favorably report H.R. 2413, as amended, to the House with the recommendation that the bill as amended do pass.

Furthermore, I move that staff be instructed to prepare the legislative report and make necessary technical and conforming amendments, and that the Chairman take all necessary steps to bring the bill before the House for consideration.

Chairman SENSENBRENNER. You have heard the motion of the gentleman from Michigan to report the bill favorably. Is there any discussion on the motion?

[No response.]

Chairman SENSENBRENNER. Hearing none, the Chair notes the presence of a reporting quorum. Those in favor will say aye.

[Chorus of ayes.]

Chairman SENSENBRENNER. Opposed, no.

[No response.]

Chairman SENSENBRENNER. The ayes appear to have it. The ayes have it, and the bill is reported favorably.

Without objection, members will have two subsequent calendar days in which to submit supplemental, minority, additional, or dissenting views on the measure.

Without objection, the bill will be reported in the form of a single amendment in the nature of a substitute reflecting amendments adopted today.

And finally, without objection, pursuant to clause 1 of Rule 22 of the Rules of the House, the Committee authorizes the Chairman to

offer such motions as may be necessary in the House to go to conference with the Senate on the bill just reported.

Without objection, these unanimous consents are agreed to.

○