105TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
105–243

COMPUTER SECURITY ENHANCEMENT ACT OF 1997

SEPTEMBER 3, 1997.—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

R E P O R T

[To accompany H.R. 1903]

[Including cost estimate of the Congressional Budget Office]

The Committee on Science, to whom was referred the bill (H.R. 1903) 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.

C O N T E N T S

I. AMENDMENT

The amendment is as follows:

Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Security Enhancement Act of 1997".

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.

(5) Federal policy for control of the export of encryption technologies should be determined in light of the public availability of comparable encryption technologies outside of the United States in order to avoid harming the competitiveness of United States computer hardware and software companies.

(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;

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

(3) provide the assessment of the capabilities of information security products incorporating cryptography that are generally available outside the United States.

SEC. 3. VOLUNTARY STANDARDS FOR PUBLIC KEY MANAGEMENT INFRASTRUCTURE.

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

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

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

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

SEC. 4. SECURITY OF FEDERAL COMPUTERS AND NETWORKS.

Section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)), as amended by section 3 of this Act, is further amended by inserting after paragraph (4), as so redesignated by section 3(1) of this Act, the following new paragraphs:

"(5) to provide guidance and assistance to Federal agencies in the protection of interconnected computer systems and to coordinate Federal response efforts related to unauthorized access to Federal computer systems;

"(6) to perform evaluations and tests of—

"(A) information technologies to assess security vulnerabilities; and

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

SEC. 5. COMPUTER SECURITY IMPLEMENTATION.

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

(1) by redesignating subsections (c) and (d) as subsections (f) and (g), 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 of Commerce in accordance with subsection (a)(4). No standards or guidelines shall be submitted to the Secretary prior to the receipt by the Institute of the Board's written recommendations. The recommendations of the Board shall accompany standards and guidelines submitted to the Secretary.

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

SEC. 7. EVALUATION OF CAPABILITIES OF FOREIGN ENCRYPTION.

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 (d), as added by section 6 of this Act, the following new subsection:

"(e)(1) If the Secretary has imposed, or proposes to impose, export restrictions on a product that incorporates encryption technologies, the Institute may accept technical evidence from the commercial provider of the product offered to indicate that encryption technologies, embodied in the form of software or hardware, that are offered and generally available outside the United States for use, sale, license, or transfer (whether for consideration or not) provide stronger participation for privacy of computer data and transmissions of information in digital form than the encryption technologies incorporated in the commercial provider's product.

"(2) Within 30 days after accepting technical evidence from a commercial provider under paragraph (1), the Institute shall evaluate the accuracy and completeness of the technical evidence and transmit to the Secretary, and to the Committee on Science of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate, a report containing the results of that evaluation. The Institute may obtain assistance from other Federal and private sector entities in carrying out evaluations under this paragraph.

"(3) Not later than 180 days after the date of the enactment of the Computer Security Enhancement Act of 1997, the Institute shall develop standard procedures and tests for determining the capabilities of encryption technologies, and shall provide information regarding those procedures and tests to the public.

"(4) The Institute may require a commercial provider seeking evaluation under this subsection to follow procedures and carry out tests developed by the Institute pursuant to paragraph (3).".

SEC. 8. 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:

"(h) 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. 9. 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 (f), 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 (f)(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 (g)(1)(B)(i), as so redesignated by section 5(1) of this Act, by inserting "and computer networks" after "computers".

SEC. 10. 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. 11. COMPUTER SECURITY FELLOWSHIP PROGRAM.

There are authorized to be appropriated to the Secretary of Commerce $250,000 for fiscal year 1998 and $500,000 for fiscal year 1999 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. 12. 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 1998, to remain available until expended, for carrying out this section.

SEC. 13. 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. 14. DIGITAL SIGNATURE INFRASTRUCTURE.

(a) NATIONAL POLICY PANEL.—The Under Secretary of Commerce for Technology shall establish a National Policy Panel for Digital Signatures. The Panel shall be composed of nongovernment and government technical and legal experts on the implementation of digital signature technologies, individuals from companies offering digital signature products and services, State officials, including officials from States which have enacted statutes establishing digital signature infrastructures, and representative individuals from the interested public.

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

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

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

(3) audit standards for certification authorities.

(c) ADMINISTRATIVE SUPPORT.—The Under Secretary of Commerce for Technology shall provide administrative support to the Panel established under subsection (a) of this section as necessary to enable the Panel to carry out its responsibilities.

SEC. 15. SOURCE OF AUTHORIZATIONS.

Amounts authorized to be appropriated by this Act shall be derived from amounts authorized under the National Institute of Standards and Technology Authorization Act of 1997.

II. PURPOSE OF THE BILL

The purpose of this 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 1997 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. 1903 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.

The need for this renewed emphasis on the security of federal civilian agencies is underscored by the General Accounting Office's (GAO) recently released High Risk Series. The series "Report on Information Management and Technology" highlighted information security as a government-wide, high-risk issue. The report stated that despite their sensitive and critical functions, federal systems and data are not being adequately protected.

Since June of 1993, the GAO has issued over 30 reports describing serious information security weaknesses at major federal agencies. In September of 1996 GAO reported that, during the previous 2 years, serious information security control weaknesses had been

reported for 10 of the 15 largest federal agencies. For half of these agencies, the weakness had been reported repeatedly for 5 years or longer.

Much has changed in the 10 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 1997 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. 1903 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.

H.R. 1903 also emphasizes the need for strong encryption. The widespread use of strong encryption will promote safety, security, and privacy.

IV. Summary of Hearings

The Subcommittee on Technology held a briefing on February 11, 1997, on the subject of secure electronic communications. The Subcommittee heard testimony from Daniel Geer, Director of Engineering, Open Market, Inc., Cambridge, Massachusetts; Daniel Lynch, Chairman, CyberCash, Redwood City, California; Tsutomu Shimomura, Senior Fellow, San Diego Supercomputing Center, La Jolla, California; Geoff Mulligan, Senior Staff Engineer, Security Products Group, SunSoft, Colorado Springs, Colorado; Daniel Farmer, Independent Security Consultant, Berkeley, California; and Eugene Spafford, Associate Professor of Computer Sciences, Purdue University, West Lafayette, Indiana.

In his testimony, Mr. Geer stressed that the conversion from a physical to an electronic world is not only well underway, but also unstoppable. He cited a need for rules to ensure and govern this new world. Before substantial investments produce diverse and conflicting interests, Congress should provide rules that are well understood and enable the "game" to develop at its own pace. Early action, by Congress, would produce the most attractive environment for the electronic world to develop. He stated that "there is really very little time remaining for Congress to itself choose whether to lead, follow or get out of the way. Where it is crucial that government lead is in setting the rules of the game." Later he went on to note: "Do not let anyone make it more complex or argue that we need to go slow or that we first have to let foreign governments or domestic law enforcement catch up. By the time that happens, you will definitely be somewhere between follow and get out of the way."

Mr. Lynch testified that the Internet system thrives like a biological element, where people add value, hopes, and ideas, then wait to see if other people like them. While considerably lowering the cost of the communication infrastructure, the Internet has also increased the visibility of activity that had once been conducted over dedicated lines. Lynch suggested the elimination of the "old laws" that protected us against the "bad guys," in order that

Internet business might flourish. He envisions the Internet as an invaluable tool for business in the future, and does not want this to be lost to foreign markets.

While providing examples of communications security problems, Mr. Shimomura testified on the inherent risks that are posed to Internet users as a result of the evolved system that currently exists. Shimomura cited, as a cause of the pernicious security problems, a failure of Internet users to recognize the fact that much of their data (stored and communicated) is at risk. The technologies to better protect users does exist; however, full-scale deployment has not yet occurred.

Mr. Mulligan discussed the three major types of security attacks: interception (where one attempts to gain valuable information by monitoring communications), intrusion (a break-in to change or steal information), and denial of service (interaction that serves to restrict the access to one's own information). In addition, he provided a summary of the primary means of protection currently available: the firewall (a perimeter defense that restricts entry access to a network, yet allows unlimited freedom once inside) and the "sandbox" (application containment that restricts certain executions from being performed by a user). Mr. Mulligan stressed that plentiful opportunities to violate communication security exist, and maintained that protection can only be ensured by "unconstrained" freedom to use any and all available security technologies.

Mr. Farmer commented on the current state of Internet security. Revisiting the widespread security compromise that was caused by the Internet Morris Worm program, Farmer stressed the need for a paradigm shift among all computer users, from a prevailing blindness to all issues of computer security, to an acceptance of the fact that one must protect his property (both physical and virtual.)

Finally, Mr. Spafford cited a lack of funding support, from both the government and industry, for educational endeavors in the area of computer security. Of the 5,500 Ph.D.s granted in computer science and engineering, a scant 16 pertained to computer security, of which only 50% were given to U.S. nationals. Mr. Spafford urged Congress to provide graduate fellowships that not only promoted the study of computer security, but also enticed the students to remain in academia upon the completion of their degree program.

On Thursday, June 19, 1997, the Subcommittee on Technology conducted a legislative hearing on H.R. 1903, the Computer Security Enhancement Act of 1997. Testimony was given by the Honorable Gary Bachula, Acting Under Secretary for Technology, Technology Administration, U.S. Department of Commerce, Washington, DC; Dr. Whitfield Diffie, Distinguished Engineer, Sun Microsystems, Mountain View, California; Mr. Stephen T. Walker, President and CEO, Trusted Information Systems, Inc., Glenwood, Maryland; Mr. James Bidzos, President and CEO, RSA Data Security, Redwood City, California; and Marc Rotenberg, Esquire, Director, Electronic Privacy Information Center, Washington, DC.

In his testimony, Mr. Bachula described an electronic world of the future, whereby one keystroke, performed by a consumer, would initiate an elaborate, electronically controlled process, resulting in the delivery of a custom good to the end user. This would require a "reliable, secure and trustworthy environment . . . We

need to have access to public information but also assurance that the wrong people will not have access to classified or private information." In addressing the sections of the bill, Mr. Bachula, speaking on behalf of the Administration, strongly supported portions of the bill that augment NIST's role in assisting the establishment of non-federal public key management infrastructures, as well as providing guidance and assistance to federal agencies. Support of Section 5 was also given. The intent of Section 6 and Section 8 was supported, yet Mr. Bachula suggested that the language needed to be improved. Mr. Bachula indicated that the Administration opposed Section 7, which gives NIST a role in the assessment of the strength of foreign encryption technologies thereby providing guidance to DoC in granting export licenses for domestic encryption products.

Mr. Diffie testified on the historical development of the government's role in computer security. In tracing the development of the interaction between National Security Agency (NSA) and NIST, Mr. Diffie spoke very highly of the intent of the Computer Security Act of 1987; however, he noted that the provision which called for NIST to consult with NSA, later modified by an inter-agency Memorandum of Understanding, resulted in a separation of authority (NIST) and funding (NSA). Mr. Diffie highlighted the problems caused by the NIST/NSA interaction, and contended that NIST autonomy would eliminate this predicament. Citing its timeliness, Mr. Diffie strongly supported H.R. 1903, which he stated would bring back the spirit of the Computer Security Act of 1987.

Mr. Walker also testified in support of H.R. 1903. He strongly supported the provisions that strengthened and augmented the role of the Computer System Security and Privacy Advisory Board (CSSPAB), which was created by the 1987 Act. He pointed out the public good that was done by CSSPAB allowing public debate on the widely criticized Clipper initiative and defended H.R. 1903's enhancement of the board's interaction with NIST. Mr. Walker, though, was opposed to the portions of the bill that direct NIST to conduct evaluations of encryption technology, both domestically (Section 4, paragraph 6) and internationally (Section 7). He questioned the ability of NIST to conduct such evaluations, not because of inadequacies of NIST, rather, the fact that "no one in government or industry has been able to perform effectively at this point" such an evaluation.

Mr. Bidzos disagreed with Mr. Walker's contention regarding evaluation of encryption technologies. He stated that the provisions of section 7 were both doable and needed. Also, Mr. Bidzos praised the bill's provisions that increased the private sector's role in establishing computer security of civilian government agencies. While implementation of the 1987 Act missed the opportunity for NIST to work closely with industry, "we have an opportunity now to correct it. And, I think that's what [H.R.] 1903 does." Concluding, Mr. Bidzos found no shortcomings with the bill, and strongly supported its contents and timing.

Mr. Rotenberg concluded oral testimony with an overall appraisal of H.R. 1903. Citing the merits of the 1987 Act, Mr. Rotenberg supported the bill as powerful and timely legislation that furthers the intent of its predecessor, while eliminating the in-

efficacy induced by NIST's Memorandum of Understanding with NSA for consultation on computer security matters under the Act.

Mr. Rotenberg stated that the Advisory Board (CSSPAB) has played a pivotal role since passage of the Computer Security Act of 1987 in providing public input into the decision-making process. He stated that he felt it appropriate to build on the success of the Board and ensure that it continues to have the resources necessary to evaluate important concerns about computer security and privacy. He made clear that the Board has played a critical role since passage of the Computer Security Act, and continues to provide the critical link between the public user community and the agency.

On the issue of Section 7 of the bill, he was extremely supportive. He stated that H.R. 1903 recognizes that the United States is not grappling with the issues of data security and privacy in a vacuum. Advanced knowledge of foreign encryption technologies would enable the Secretary of Commerce to analyze export restrictions while possessing a firm understanding of the availability of strong foreign encryption products.

He expressed the hope that an awareness of technologies available outside the United States will influence decision-makers to adopt a policy on encryption that will help U.S. computer hardware and software manufacturers to be competitive in what is essentially a global market. It is simply not wise to make recommendations without consideration of the full range of relevant data.

He testified that the experience with the Digital Signature Standard confirms his belief that the best technological development is driven by openness and public accountability. He stated that H.R. 1903 creates a framework that will ensure a responsive, open decision-making process that will promote technical standards compatible with the interests of civilian agencies and the commercial sector.

Finally, Mr. Rotenberg complimented the National Research Council's (NRC's) work in reviewing cryptography policy in the 1996 Cryptography's Role In Securing The Information Society report, and suggested that the proposed study (Section 12) be expanded to include: "new techniques to promote privacy and security on-line, techniques to promote anonymous or pseudo-anonymous commerce, and communications that are now being explored in other countries."

He stated that it is very important for the NRC to look at privacy enhancing technologies that may enable the growth of electronic commerce on the Internet and strengthen public confidence in Internet communication. Similar work has been carried out in other countries, but the United States has still not looked closely at the significant opportunities that such technologies provide. A report from the NRC, setting out the basic research and policy issues with some preliminary recommendations, would be very useful.

In addition, Mr. Willis Ware submitted written testimony for the record on behalf of the Computer System Security and Privacy Advisory Board (CSSPAB), which he chairs. In reviewing the 1987 Computer Security Act 10 years after its enactment, CSSPAB heard presentations from a variety of government and private sector representatives who criticized the Act's implementation, rather

than its structure or wording. For example, Mr. Ware noted that NIST is not providing federal civilian agencies the support they need to ensure computer security. Ware stated that NIST should focus on providing "general system-level security advice and overall assistance to civil agencies," not just technical assistance in implementing standards and guidelines. In June 1997, CSSPAB adopted two resolutions. The first calls for NIST to increase its assistance to civilian federal agencies. The second recommends that NIST develop a repository for data from civilian agencies on computer security and privacy violations.

V. Committee Actions

On Monday, July 29, 1997, the Committee on Science, Subcommittee on Technology convened to mark up H.R. 1903, The Computer Security Enhancement Act of 1997, 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. Two amendments were offered at the markup. Both amendments were adopted by voice vote.

1. Mrs. Morella offered an amendment to increase the amount of funding for the Computer Security Fellowships Program, as administered by the National Institute of Standards and Technology, from $250,000 to $500,000 in Fiscal Year 1999. The amendment was adopted by a voice vote.

2. Mr. Gordon offered an amendment to further increase public awareness of security threats and to accelerate corrective action by using the Technology Administration in the Commerce Department to actively promote greater use of cryptography and associated technologies by the private sector. The amendment also establishes a national forum for coordination of policies for building a digital signature infrastructure by establishing a national panel, under the auspices of the Technology Administration, to develop model practices and procedures, uniformity among jurisdictions that license certification authorities, and uniform audit standards for certification authorities. The amendment was adopted by a voice vote.

With a quorum present, Mr. Gordon moved that H.R. 1903, as amended, be reported. The motion was adopted by a voice vote.

On July 29, 1997, the Committee on Science convened to mark up H.R. 1903. An amendment by Representatives Morella and Gordon was offered and adopted by voice vote.

1. Mrs. Morella and Mr. Gordon offered an amendment which consisted of the text of H.R. 1903 as reported by the Subcommittee on Technology. The amendment was agreed to by a voice vote.

With a quorum present, Mr. Gordon moved that H.R. 1903, as amended, be reported. The motion was adopted by a voice vote.

VI. Summary of Major Provisions of the Bill

The Computer Security Enhancement Act of 1997 updates the Computer Security Act to take into account the evolution of computer networks and their use by both the Federal Government and the private sector. Specifically, H.R. 1903:

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

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

3. Requires NIST to develop standard tests and procedures to determine the capabilities of encryption technologies. Through such tests and procedures, NIST may assist private sector entities, by request, in evaluating the relative strength of foreign encryption products, thereby defusing some of the concerns associated with the export of domestically produced encryption products.

4. The bill 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.

5. 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.

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

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

8. 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.

9. 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.

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

SECTION 1. SHORT TITLE

Cites this title as the "Computer Security Enhancement Act of 1997."

SECTION 2. FINDINGS AND PURPOSES

The Committee finds:

(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 the 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.

(5) Federal policy for control of the export of encryption technologies should be determined in light of the public availability of comparable encryption technologies outside of the United States in order to avoid harming the competitiveness of United States computer hardware and software companies.

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;

(2) promote technology solutions based on private sector offerings to protect the security of federal computer systems; and

(3) provide the assessment of capabilities of information security products incorporating cryptography that are generally available outside the United States.

SECTION 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.

SECTION 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 and coordinate federal response efforts related to unauthorized access to federal computer systems; and

(2) perform evaluations and tests of information technologies to assess security vulnerabilities and of commercially available security products for their suitability for use by federal agencies for protecting sensitive information in computer systems.

Committee views

The Committee continues to support NIST's role in evaluating the products used for information technology security for the federal civilian agencies. 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. To do this, NIST must evaluate and perform tests to determine which of the commercially available security products available are the least vulnerable and the best suited to protect electronic data.

SECTION 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. Specifically, NIST must emphasize technology-neutral policy guidelines for computer security practices, and must actively promote commercially available products for meeting the security and privacy requirements of federal agencies. Also, NIST is tasked to participate in implementations of encryption technologies to develop necessary standards and guidelines for federal computer systems, including assessing the desirability of, and the costs associated with, establishing and managing a key recovery infrastructure.

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.

The Committee is not convinced of the necessity of the establishment of a national key management infrastructure. In the process of looking at a national key management infrastructure it is also necessary to examine whether one is needed at all. The Committee believes more information is needed about the costs and vulnerabilities of key management infrastructures. The NRC study will provide valuable information on the costs and vulnerabilities of such an infrastructure. The Committee expects NIST to partici-

pate in the implementation of encryption technologies in the Federal Government, including assessment of the desirability of, and the costs associated with, establishing and managing key recovery infrastructures for Federal Government information.

SECTION 6. COMPUTER SECURITY REVIEW, PUBLIC MEETINGS, AND INFORMATION

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

SECTION 7. EVALUATION OF CAPABILITIES OF FOREIGN ENCRYPTION

Section 20 of the NIST Act is amended to enable NIST to accept technical information from commercial encryption providers whose products are the subject of export restrictions demonstrating that stronger encryption products than their own already exist outside the United States. NIST is then required to analyze the information and within 30 days provide a report on its accuracy and completeness to the Secretary of Commerce and Congress.

In order to facilitate the evaluation process, within 180 days of enactment of this Act, NIST is required to develop standard procedures and tests to measure the capabilities of encryption technologies. NIST must make information regarding those procedures

and tests available to the public. NIST is given the authority to require commercial providers seeking an evaluation to follow the procedures and tests it has developed.

Committee views

NIST currently assesses domestic products in its mission to set appropriate federal standards and to assist civilian federal agencies in the area of computer security. By directing NIST to develop standard procedures and tests that can be used by commercial encryption providers whose products are the subject of export restrictions to evaluate the strength of foreign encryption, the bill will allow the Administration and Congress to make informed decisions on criteria for exporting U.S. encryption products.

The Committee believes that providing accurate and verifiable information on the availability of strong security products will also assist U.S. companies to remain competitive in the international market.

SECTION 8. 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.

SECTION 9. 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.

SECTION 10. 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 networked 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 networked information technology programs which raise unique security concerns.

SECTION 11. 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 ($250,000 for Fiscal Year 1998 and $500,000 for Fiscal Year 1999).

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.

SECTION 12. STUDY OF PUBLIC KEY INFRASTRUCTURE BY THE NATIONAL RESEARCH COUNCIL

This section authorizes funds ($450,000 for Fiscal Year 1998 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 for use by individuals, businesses, and government.

Committee views

In the opinion of the Committee, the NRC study on Cryptography "Cryptography's Role In Securing the Information Society" has been an important addition to the cryptography debate. The issues arising from the debate of public key infrastructures could similarly benefit from an NRC report.

SECTION 13. 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 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 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 13, 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 net-

works. 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. 1903 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 13 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.

SECTION 14. DIGITAL SIGNATURE INFRASTRUCTURE

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 market driven consensus 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. 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. Other-

wise, 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 14 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 legal and technical infrastructure that is a prerequisite for the widespread use of digital signatures.

SECTION 15. SOURCE OF AUTHORIZATIONS

Amounts authorized to be appropriated by this Act are from amounts authorized by the NIST Authorization Act of 1997.

Committee views

The Committee and the full House of Representatives have passed H.R. 1274, the National Institute of Standards and Technology Authorization Act of 1997. That bill includes authorizations which, if enacted, are sufficient to cover all responsibilities given to NIST in H.R. 1903.

VIII. COMMITTEE COST ESTIMATE

Clause 7(a) of rule XIII of the Rules 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 5 fiscal years following such fiscal year (or for the authorized duration of any program authorized by such bill or joint resolution, if less than 5 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, clause 7(d) of that Rule provides that this requirement does not apply when a cost estimate and comparison prepared by the Director of the Congressional Budget Office under section 403 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 clause 2(l)(3)(C) of rule XI. A cost estimate and comparison prepared by the Director of the Congressional Budget Office under section 403 of the Congressional Budget Act of 1974 has been timely submitted prior to the filing of this report and included in Section XI of this report pursuant to clause 2(l)(3)(C) of rule XI.

Clause 2(l)(3)(B) of rule XI of the Rules of the House of Representatives requires each Committee report that accompanies a measure providing new budget authority (other than continuing ap-

propriations), 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. 1903 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. 1903 does authorize additional discretionary spending, as described in the Congressional Budget Office report on the bill, which is contained in Section XI of this report.

IX. Congressional Budget Office Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, August 12, 1997.

Hon. F. James Sensenbrenner, Jr.,
Chairman, Committee on Science,
U.S. House of Representatives,
Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 1903, the Computer Security Enhancement Act of 1997.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Rachel Forward, who can be reached at 226–2860.

Sincerely,

June E. O'Neill

Enclosure

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

Summary: H.R. 1903 would direct the National Institute of Standards and Technology (NIST) located in the Department of Commerce to develop policies to improve computer security for federal computer systems. CBO estimates that implementing the bill would cost $35 million over the 1998–2002 period, assuming appropriation of the necessary amounts.

The bill would authorize the appropriation of $3.2 million to NIST to (1) enable the Computer System Security and Privacy Advisory Board (CSSPAB) administered by NIST to conduct public forums to identify emerging issues related to computer security, (2) contract for a study by the National Research Council on computer security issues, and (3) award computer security fellowships. In addition, CBO estimates that implementing other provisions of the bill would require expenditures of about $33 million over the 1998–2002 period.

H.R. 1903 would not affect direct spending or receipts; therefore, pay-as-you go procedures would not apply. H.R. 1903 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act of 1995 (UMRA) and would not affect the budgets of state, local, or tribal governments.

Estimated cost to the Federal Government: For the purposes of this estimate, CBO assumes that H.R. 1903 will be enacted by the end of Fiscal Year 1997, and that the estimated amounts necessary to implement the bill will be appropriated by the start of each fiscal year. Outlays have been estimated on the basis of historical spending patterns for NIST and information provided by the agency. The estimated budgetary impact of H.R. 1903 is shown in the following table.

CHANGES IN SPENDING SUBJECT TO APPROPRIATION

[By fiscal year, in millions of dollars]

	1998	1999	2000	2001	2002
Estimated Authorization Level	9	8	7	6	6
Estimated Outlays	7	8	7	7	6

NIST received an appropriation of $582 million for Fiscal Year 1997, and its 1997 outlays are estimated to be about $640 million.

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

BASIS OF ESTIMATE

Based on information from NIST, CBO estimates that enacting H.R. 1903 would result in total costs to the government of about $35 million over the 1998–2002 period. Of that amount, $3.2 million is specifically authorized in the bill for the activities of the CSSPAB and the National Research Council, as well as for the computer security fellowship program at NIST.

CBO estimates that NIST would need additional appropriations of $6 million to $7 million in each fiscal year over the 1998–2002 period to implement the remaining provisions of the bill. Of those amounts, CBO estimates that NIST would spend about $5 million a year to evaluate commercial encryption products subject to export restrictions and to report the results to the Secretary of Commerce and the Congress. We further estimate that NIST would spend between $1 million and $2 million in each year to test computer security products for use by federal agencies, provide information on computer security threats to the public, establish a National Panel for Digital Signatures, and carry out the remaining provisions of the bill.

H.R. 1903 directs that the sums necessary to implement this bill, including the $3.2 million explicitly authorized by the bill, should be derived from amounts authorized to be appropriated in H.R. 1274, the National Institute of Standards and Technology Authorization Act of 1997. That act has been passed by the House of Representatives but has not yet been enacted into law.

Pay-as-you-go considerations: None.

INTERGOVERNMENTAL AND PRIVATE-SECTOR IMPACT

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

Estimate prepared by: Rachel Forward (226–2860).

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

X. Compliance With Public Law 104–4

H.R. 1903 contains no unfunded mandates.

XI. Committee Oversight Findings and Recommendations

Clause 2(l)(3)(A) of rule XI of the Rules 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 has no oversight findings.

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

Clause 2(l)(3)(D) of rule XI of the Rules 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 and Oversight 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 and Oversight.

XIII. Constitutional Authority Statement

Clause 2(l)(4) of rule XI of the Rules 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. 1903.

XIV. Federal Advisory Committee Statement

The functions of the two advisory committees, the Computer System Security and Privacy Advisory Board and the National Panel for Digital Signatures, authorized in H.R. 1903 are not currently, nor could they be, performed by one or more agencies or by enlarging the mandate of another existing advisory committee.

XV. Congressional Accountability Act

The Committee finds that H.R. 1903 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. Changes in Existing Law Made by the Bill, as Reported

In compliance with clause 3 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 italics, 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 Information Technology Management Reform Act of 1996;

[(3)**]** *(4)* to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987;

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

(6) to perform evaluations and tests of—

(A) information technologies to assess security vulnerabilities; and

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

[(4)**]** *(7)* to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost-effective security and privacy of sensitive information in Federal computer systems; and

[(5)**]** *(8)* to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget) *to the extent that such coordination will improve computer security and to the extent necessary for improving such security for Federal computer systems*—

(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a) (3) and (5)

are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

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

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

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

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

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

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

(e)(1) If the Secretary has imposed, or proposes to impose, export restrictions on a product that incorporates encryption technologies, the Institute may accept technical evidence from the commercial provider of the product offered to indicate that encryption technologies, embodied in the form of software or hardware, that are offered and generally available outside the United States for use, sale, license, or transfer (whether for consideration or not) provide stronger participation for privacy of computer data and transmissions of information in digital form than the encryption technologies incorporated in the commercial provider's product.

(2) Within 30 days after accepting technical evidence from a commercial provider under paragraph (1), the Institute shall evaluate the accuracy and completeness of the technical evidence and transmit to the Secretary, and to the Committee on Science of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate, a report containing the results of that evaluation. The Institute may obtain assistance from other Federal and private sector entities in carrying out evaluations under this paragraph.

(3) Not later than 180 days after the date of the enactment of the Computer Security Enhancement Act of 1997, the Institute shall develop standard procedures and tests for determining the capabilities of encryption technologies, and shall provide information regarding those procedures and tests to the public.

(4) The Institute may require a commercial provider seeking evaluation under this subsection to follow procedures and carry out tests developed by the Institute pursuant to paragraph (3).

[(c)] *(f)* For the purposes of—

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

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

the Institute [shall draw upon] *may draw upon* computer system technical security guidelines developed by the National Security Agency to the extent that the Institute determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

[(d)] *(g)* As used in this section—

(1) the term "computer system"—

(A) * * *

(B) includes—

(i) computers *and computer networks*;

* * * * * * *

(h) 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.

* * * * * * *

XVII. COMMITTEE RECOMMENDATIONS

On July 29, 1997, a quorum being present, the Committee favorably reported The Computer Security Enhancement Act of 1997 by a voice vote and recommends its enactment.

XVIII. PROCEEDINGS OF SUBCOMMITTEE MARKUP

SUBCOMMITTEE MARKUP OF H.R. 1903—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

MONDAY, JULY 28, 1997

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

The Subcommittee met at 4:10 p.m., in room 2318 of the 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.

Pursuant to notice, the Subcommittee on Technology is meeting today to consider the following measure: H.R. 1903, the Computer Security Enhancement Act of 1997.

I would ask unanimous consent for the authority to recess.

[No response.]

Chairwoman MORELLA. No objection? I think someone needs to move that we have the authority to recess, just in case. We do not anticipate it.

Mr. EHLERS. So moved.

Chairwoman MORELLA. Thank you. It has been so moved. No objection?

[No response.]

Chairwoman MORELLA. I thank you very much.

I will proceed with some opening comments that deal with the nature of the bill that we have before us that we are going to be marking up.

I want to commend my colleagues, first of all, who have helped in crafting H.R. 1903: the Ranking Member of the Subcommittee on Technology, Bart Gordon; the Chairman of the Full Committee, Jim Sensenbrenner; Ranking Member of the Full Committee, George Brown; and the rest of the original co-sponsors.

It is very impressive. We currently have 25 co-sponsors on the bill, 24 of them from the Committee. I want to especially thank my

fellow Subcommittee members for co-sponsoring H.R. 1903: Mr. Davis, Ms. Stabenow, Mr. Ehlers, Mr. Cook, Mr. Cannon, Mr. Gutknecht, Mr. Brady, Ms. Tauscher, Mr. Weldon, Mr. Doyle, Mr. Barcia, Mr. Ewing, and Mr. Bartlett and Ms. Rivers. The list includes all of the Subcommittee Republicans and just about all of the Democrats.

The Computer Security Enhancement Act will strengthen the National Institute of Standards and Technology's historic role established by the Computer Security Act of 1987 in setting standards for computer security at federal and civilian agencies.

The bill updates the decade-old Act while giving NIST the tools it requires to ensure that appropriate attention and effort is concentrated on securing our federal information technology infrastructure.

We all know the need for these changes is great. Today we are faced with a world where telecommunications' services retailing in the electric power grid are all dependent on large networked computer systems.

This dependence has allowed us an incredible amount of flexibility, spurred an extraordinary increase in productivity, and improved the very way that we conduct business.

The extraordinary success in technological advances in computing power is a double-edged sword. On the one hand, as the cost of computer power plummets, cryptographic systems that once offered adequate protection for data become insecure.

On the other hand, these advances will allow users to secure information more inexpensively and more effectively with encryption and firewalls.

The Federal Government's dependence in computer systems' networks and electronic records has grown tremendously in the last decade.

Information systems are now integral to nearly every aspect of over $1.5 trillion in annual Federal Government operations and spending. And yet, despite years of experience in developing systems, agencies across the government continue to have chronic problems ensuring the security of their information technology system.

The bottom line is that theft or corruption of proprietary data is a real threat to our national security. Not withstanding the reluctance to disclose details of security compromises or related losses, some estimates of the extent of financial fraud in security-related attacks have been assembled.

Information Week in August of 1995 reported on-line information theft, including calling card and credit card numbers, pirated software and corporate secrets, totalling $10 billion annually in the United States alone.

Ernst & Young in their Third Annual Information Security Survey for 1996 stated that nearly 50 percent of organizations suffered an information security-related financial loss in the last 2 years.

This survey went on to state that 10 percent of users reported an attempted or successful break-in to their system via the Internet in the past year. Even more alarming is their discovery that over 50 percent of those surveyed claimed they would not know if someone broke into their systems through the Internet.

And according to the July 1995 issue of Open Computing, 20 percent of organizations that have external network access have been hacked.

The risks inherent in electronic commerce can only be mitigated by the use of appropriate security countermeasures in conjunction with the establishment of the necessary business and legal frameworks.

So H.R. 1903 will help address these issues by promoting a more secure information technology network in the federal civilian agencies and assisting American companies in their efforts to protect private systems.

The Computer Security Enhancement Act of 1997 accomplishes these goals by updating the Computer Security Act to take into account the evolution of computer networks and their increased use by both the Federal Government and the private sector.

So specifically the bill will:

Number one, require NIST to encourage the acquisition of off-the-shelf products to meet civilian agency computer security needs. This measure should reduce the cost and improve the availability of computer security technologies for federal agencies.

Second, the bill increases the input of the Independent Computer System Security and Privacy Advisory Board into NIST's decision-making process. The Board, which is made up of representatives from industry, federal agencies, and other external organizations, should assist NIST in its developments of standards and guidelines for federal systems.

Thirdly, the bill requires NIST to develop standardized tests and procedures to evaluate the strength of foreign encryption products. Through such tests and procedures, NIST with assistance from the private sector, will be able to judge the relative strength of foreign encryption, thereby defusing some of the concerns associated with the export of domestically produced encryption products.

Fourth, the bill limits NIST's involvement to the development of standards and guidelines for federal civilian systems. The bill clarifies the NIST's standards and guidelines are to be used for the acquisition of security technologies for the Federal Government and are not intended as restrictions on the production or use of encryption by the private sector.

Also, the bill updates the Computer Security Act to address changes in technology over the last decade. Significant changes in the manner in which information technology is used by the Federal Government have occurred since the enactment of the Computer Security Act. So this bill updates the Act by including references to computer networking which has become an increasingly important component of the Federal Government's information technology system.

The bill also establishes a new Computer Science Fellowship Program for graduate and undergraduate students studying computer security. It sets aside $250,000 a year for each of the next 2 fiscal years to enable NIST to finance computer security fellowships under an existing NIST grant program.

The bill also requires the National Research Council to conduct a study to assess the desirability of public key infrastructures. The

NRC would also research the technologies required for the establishment of such key infrastructures.

I am personally committed to increasing awareness on issues of information technology security, and this Subcommittee has held three briefings and hearings on the issue; has met with scores of knowledgeable experts in the field; and so I am pleased to be one of the original co- sponsors on H.R. 1903.

I thank all of the members who are here today for their staunch support.

I would now like to recognize the Distinguished Ranking Member of the Subcommittee on Technology, Mr. Gordon.

Mr. GORDON. Thank you.

Chairwoman Morella has explained the provisions of H.R. 1903. Many of us are co-sponsors of this legislation; therefore, I will keep my statement very brief.

I want to highlight the underlying purpose of this legislation: to encourage the use of encryption products both by the Federal Government and the private sector.

I am convinced that we must have a trustworthy and secure electronic network system to foster the growth of electronic commerce.

Although many might consider this a piece of esoteric legislation, it is not. The issue of computer security and privacy in electronic networks and the Internet is a pressing issue for every American.

This week there was an article on the Internet on privacy not in The Wall Street Journal or Business Week or PC World, but in People Magazine.

The overall conclusion of the article was that most people simply are not aware of the need to secure information on the Net, or how easily accessible information is unless appropriate precautions are taken.

This bill builds on the successful track record of the National Institute of Standards and Technology in working with industry and other federal agencies to develop a consensus on the necessary standards and protocols required for electronic commerce.

I intend to offer an amendment which will further strengthen this legislation by including a government-industry partnership to begin to address the issue of digital signatures, something that should have been started 2 or 3 years ago.

This legislation is consistent with recommendations to the Office of Technology Assessment, the National Research Council, and independent experts who have appeared before this Subcommittee.

Finally, the underlying principle of H.R. 1903 is that it recognizes that the Government and private sector security needs are similar. Hopefully the result will be lower cost and better security for everyone.

This bill is the result of bipartisan cooperation and it has been a pleasure working with Chairwoman Morella on this issue.

I urge my colleagues to support this legislation.

Chairwoman MORELLA. Thank you, Mr. Gordon.

Do we have any other members who would like to offer any opening statements?

[No response.]

Chairwoman MORELLA. Hearing none, I ask unanimous consent that the bill be considered as read and open to amendment at any point.

[No response.]

Chairwoman MORELLA. I would ask members to proceed with the amendments in the order of the roster.

I have an amendment which the Clerk will report.

Mr. BELL. Amendment to H.R. 1903 offered by Mrs. Morella:

"Page 10, line 8, strike '$250,000' and insert in lieu thereof '$500,000.'"

Chairwoman MORELLA. This amendment will allow an increase so that NIST can continue funding in Fiscal Year 1999 fellowships that were begun in Fiscal Year 1998, while still allowing for new candidates to begin fellowships in Fiscal Year 1999.

It is my understanding that the amendment has been cleared by the Minority and is noncontroversial.

Is there any discussion on that amendment?

Yes, Mr. Bartlett?

Mr. BARTLETT. Madam Chairwoman, do we need an offset for this? Or will they simply provide the funds by reprogramming within the agency?

Chairwoman MORELLA. Yes. My understanding, and we tried to work this out with regard to the amendment, is that the offset is within the bill itself. The money is already there, so it does not require any additional money.

Mr. BARTLETT. Thank you, very much.

Chairwoman MORELLA. Does everybody approve of the amendment?

[No response.]

Chairwoman MORELLA. If there is no further discussion on the amendment, then the vote occurs on the amendment.

All in favor will designate by saying, aye.

[Chorus of ayes.]

Chairwoman MORELLA. Opposed?

[No response.]

Chairwoman MORELLA. The ayes have it unanimously.

I note that there is another amendment, Mr. Gordon. I will recognize you for an amendment.

Mr. GORDON. Madam Chairwoman, I have an amendment at the desk.

Chairwoman MORELLA. All right. The Clerk will read the amendment.

Mr. BELL. "Amendment to H.R. 1903 offered by Mr. Gordon:

"Page 12, after line 11"

Mr. GORDON. Madam Chairwoman, I move that we dispense with the reading of the amendment.

Chairwoman MORELLA. So moved.

Mr. GORDON. Madam Chairwoman, I will just give a brief overview of the purpose of this amendment. I understand that you intend to support this amendment and the staff have been working together.

This amendment adds two additional provisions to H.R. 1903.

First, it increases public awareness of the need for improving the security of communications networks by including a requirement

that the Technology Administration establish a clearinghouse of public information on electronic security threats.

Second, it establishes a coordination mechanism in the development of a national digital signature infrastructure by establishing a national panel of state, business, and technical legal experts.

I became interested in this issue of digital signature technology as a result of press articles on the electronic commerce and the fact that States are beginning to regulate this aspect of electronic commerce.

If we are to create a seamless electronic network, then we need uniform rules of the road. Digital signature technology is essential to ensuring public trust of networks such as the Internet.

Digital signature verifies that the business or individual you are communicating with is who you think they are, and that the information being exchanged has not been altered in transit.

For this technology to be developed, a trusted guarantor of the digital signature must exist such as a certification authority.

Several States already have statutes in place to regulate certification authorities. However, for a national system to develop, uniform standards must be in place for the practices and procedures of certification.

Without this national uniformity, variations will exist among different state requirements for certification authorities which could affect the reliability and security of the operations associated with issuing and managing certifications.

This amendment does not give the Federal Government the authority to establish standards or procedures. This amendment creates a national panel of public and private representatives to begin to address how to develop and integrate national policy regarding digital signatures.

It is entirely consistent with the recommendations of the National Academy of Science study and the testimony of witnesses at our June 19th hearings.

I urge my colleagues to support this amendment.

Chairwoman MORELLA. I would like to comment that I do support the Gordon Amendment to H.R. 1903. It strives to promote uniformity in the formation of digital signature standards by establishing a national panel under the auspices of the Technology Administration.

While having no authority to develop standards governing the private sector, the panel does provide for a formal structure that ensures policies critical for the widespread use of digital signatures.

I am pleased that Mr. Gordon has offered this amendment. I support it.

I wonder, is there any further discussion on the Gordon amendment?

[No response.]

Chairwoman MORELLA. Hearing none, then, the vote will occur on the amendment.

All in favor will designate, aye.

[Chorus of ayes.]

Chairwoman MORELLA. Opposed?

[No response.]

Chairwoman MORELLA. Hearing no opposition, the amendment is reported unanimously favorably.

Are there any further amendments that members seek to offer?

[No response.]

Chairwoman MORELLA. Hearing none then the question is on the bill, on H.R. 1903, the Computer Security Enhancement Act of 1997, as amended.

All those in favor will designate by, aye.

[Chorus of ayes.]

Chairwoman MORELLA. Opposed, no?

[No response.]

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

I would like to recognize the Honorable Ranking Member, Bart Gordon, for a motion.

Mr. GORDON. Madam Chairwoman, I move the Subcommittee report the bill, H.R. 1903, as amended, and that the Chairwoman take all necessary steps to bring the bill before the Full Committee for consideration.

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

[Chorus of ayes.]

Chairwoman MORELLA. 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.

This concludes our Subcommittee markup on H.R. 1903. The Chair declares the Subcommittee adjourned and thanks all of the members for their wonderful attendance.

[Whereupon, at 4:27 p.m., Monday, July 28, 1997, the markup was adjourned.]

XIX. PROCEEDINGS OF FULL COMMITTEE MARKUP

FULL COMMITTEE MARKUP OF H.R. 1903—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

TUESDAY, JULY 29, 1997

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

The Committee met at 1:10 p.m., in room 2318 of the Rayburn House Office Building, Hon. F. James Sensenbrenner, Jr., Chairman of the Committee, presiding.

Chairman SENSENBRENNER. The Committee will come to order.

Pursuant to notice, the Committee on Science is meeting today to consider the following measures:

H.R. 1903, the Computer Security Enhancement Act of 1997, As amended;

H.R. 2249, To Authorize Appropriations for Carrying Out The Earthquake Hazards Reduction Act of 1977 For Fiscal Years 1997, 1998 and 1999, and For Other Purposes; and

H.R. 922, the Human Cloning Research Prohibition Act.

I ask unanimous consent for the Chair to declare authority to recess during votes.

[No response.]

Chairman SENSENBRENNER. Without objection, so ordered.

I am informed that the Democrats have all been invited to go down to the White House to celebrate the balanced budget. I know that is something they really ought to do because it is really new for them.

So I am going to forego opening statements. I would request all of the members to forego opening statements, particularly those on my side of the aisle, because I think if they get in the mood of celebrating balanced budgets, then we can stick to this agreement for the next 5 fiscal years and actually get the balanced budget.

So the first bill up, since there are going to be no opening statements so that can happen, will be H.R. 1903, the Computer Security Enhancement Act of 1997.

I ask unanimous consent that the bill be considered as read and open for amendment at any point.

[The text of the bill and supporting materials follow:]

I

105TH CONGRESS
1ST SESSION

H. R. 1903

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

JUNE 17, 1997

Mr. SENSENBRENNER (for himself, Mr. BROWN of California, Mrs. MORELLA, Mr. GORDON, Mr. DAVIS of Virginia, Ms. STABENOW, Mr. EHLERS, Ms. JACKSON-LEE of Texas, Mr. SESSIONS, Mr. PICKERING, Mr. TRAFICANT, Mr. COOK, and Mr. CANNON) 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 1997".

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.

(5) Federal policy for control of the export of encryption technologies should be determined in light of the public availability of comparable encryption technologies outside of the United States in order to avoid harming the competitiveness of United States computer hardware and software companies.

(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;

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

(3) provide the assessment of the capabilities of information security products incorporating cryptography that are generally available outside the United States.

SEC. 3. VOLUNTARY STANDARDS FOR PUBLIC KEY MANAGEMENT INFRASTRUCTURE.

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

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

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

"(2) upon request from the private sector, to assist in establishing voluntary interoperable standards, guidelines, and associated methods and techniques to facilitate and expedite the establishment of non-Federal management infrastructures for public

keys that can be used to communicate with and conduct transactions with the Federal Government;".

SEC. 4. SECURITY OF FEDERAL COMPUTERS AND NETWORKS.

Section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(b)), as amended by section 3 of this Act, is further amended by inserting after paragraph (4), as so redesignated by section 3(1) of this Act, the following new paragraphs:

"(5) to provide guidance and assistance to Federal agencies in the protection of interconnected computer systems and to coordinate Federal response efforts related to unauthorized access to Federal computer systems;

"(6) to perform evaluations and tests of—

"(A) information technologies to assess security vulnerabilities; and

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

SEC. 5. COMPUTER SECURITY IMPLEMENTATION.

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

(1) by redesignating subsections (c) and (d) as subsections (f) and (g), 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 of Commerce in accordance with subsection (a)(4). No standards or guidelines shall be submitted to the Secretary prior to the receipt by the Institute of the Board's written recommendations. The recommendations of the Board shall accompany standards and guidelines submitted to the Secretary.

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

SEC. 7. EVALUATION OF CAPABILITIES OF FOREIGN ENCRYPTION.

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 (d), as added by section 6 of this Act, the following new subsection:

"(e)(1) If the Secretary has imposed, or proposes to impose, export restrictions on a product that incorporates encryption technologies, the Institute may accept technical evidence from the commercial provider of the product offered to indicate that encryption technologies, embodied in the form of software or hardware, that are offered and generally available outside the United States for use, sale, license, or transfer (whether for consideration or not) provide stronger participation for privacy of computer data and transmissions of information in digital form than the encryption technologies incorporated in the commercial provider's product.

"(2) Within 30 days after accepting technical evidence from a commercial provider under paragraph (1), the Institute shall evaluate the accuracy and completeness of the technical evidence and transmit to the Secretary, and to the Committee on Science of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate, a report containing the results of that evaluation. The Institute may obtain assistance from other Federal and private sector entities in carrying out evaluations under this paragraph.

"(3) Not later than 180 days after the date of the enactment of the Computer Security Enhancement Act of 1997, the Institute shall develop standard procedures and tests for determining the capabilities of encryption technologies, and shall provide information regarding those procedures and tests to the public.

"(4) The Institute may require a commercial provider seeking evaluation under this subsection to follow procedures and carry out tests developed by the Institute pursuant to paragraph (3).".

SEC. 8. 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:

"(h) 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. 9. 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 (f), 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 (f)(2), as so redesignated by section 5(1) of this Act, by striking "(b)(5)" and inserting in lieu thereof "(b)(5)"; and

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

SEC. 10. 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. 11. COMPUTER SECURITY FELLOWSHIP PROGRAM.

There are authorized to be appropriated to the Secretary of Commerce $250,000 for fiscal year 1998 and $250,000 for fiscal year 1999 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. 12. 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 1998, to remain available until expended, for carrying out this section.

SEC. 13. SOURCE OF AUTHORIZATIONS.

Amounts authorized to be appropriated by this Act shall be derived from amounts authorized under the National Institute of Standards and Technology Authorization Act of 1997.

○

H.R. 1903
Computer Security Enhancement Act of 1997

Section-by-Section Summary

SEC. 1. Short Title.

Computer Security Enhancement Act of 1997.

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.

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 and coordinate federal response efforts related to unauthorized access to federal computer systems; and

(2) perform evaluations and tests of information technologies to assess security vulnerabilities and of commercially available security products for their suitability for use by federal agencies for protecting sensitive information in computer systems.

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. Specifically, NIST must emphasize technology-neutral policy guidelines, and must actively promote commercially available products for meeting the security and privacy requirements of federal agencies. Also, NIST is tasked to participate in implementations of encryption technologies to develop necessary standards and guidelines for federal computer systems, including assessing the desirability of and the costs associated with establishing and managing a key recovery infrastructure.

48

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 ($1,000,000 for FY 1998 and $1,030,000 for FY 1999) to enable it to act as a forum for public discussion on emerging issues related to computer security, privacy and cryptography. The Board is authorized to convene public meetings and to publish reports and other information for public distribution.

SEC. 7. Evaluation Of Capabilities of Foreign Encryption.

Section 20 of the NIST Act is amended to enable NIST to accept technical information from commercial encryption providers whose products are the subject of export restrictions demonstrating that stronger encryption products than their own already exist outside the United States. NIST is then required to analyze the information and within 30 days provide a report on its accuracy and completeness to the Secretary of Commerce and Congress.

In order to facilitate the evaluation process, within 180 days of enactment of the act, NIST is required to develop standard procedures and tests to measure the capabilities of encryption technologies. NIST must make information regarding those procedures and tests available to the public. NIST is given the authority to require commercial providers seeking an evaluation to follow the procedures and tests it has developed.

SEC. 8. 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.

SEC.9. 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.

SEC.10. 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.

SEC. 11. Computer Security Fellowship Program.

49

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 ($250,000 for FY 1998 and FY 1999).

SEC. 12. Study of Public Key Infrastructure by the National Research Council.

This section authorizes funds ($450,000 for FY 1998 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 for use by individuals, businesses, and government.

SEC. 13. Source of Authorizations.

Amounts authorized to be appropriated by this Act are from amounts authorized by the NIST Authorization Act of 1997.

50

Highlights of H.R. 1903, The Computer Security Enhancement Act of 1997

The Computer Security Enhancement Act of 1997 will strengthen the National Institute of Standards and Technology's (NIST's) historic role in computer security established by the Computer Security Act of 1987 (P.L.100-235). The bill updates 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.

The Computer Security Act of 1987 gave NIST the lead responsibility for computer security for Federal civilian agencies. The act requires NIST to develop the standards and guidelines needed to ensure cost-effective security and privacy of sensitive information in Federal computer systems.

The Computer Security Enhancement Act of 1997 updates the Computer Security Act to take into account the evolution of computer networks and their use by both the Federal Government and the private sector. Specifically, the security enhancement act:

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

2. Increases the input of the independent Computer System Security and Privacy Advisory Board into NIST's decision-making process. The board, which is made up of representatives from industry, federal agencies and other external organizations, should assist NIST in its development of standards and guidelines for Federal systems.

3. Requires NIST to develop standardized tests and procedures to evaluate the strength of foreign encryption products. Through such tests and procedures, NIST, with assistance from the private sector, will be able to judge the relative strength of foreign encryption, thereby defusing some of the concerns associated with the export of domestically produced encryption products.

4. Limits NIST's involvement to the development of standards and guidelines for Federal civilian systems. The bill clarifies that NIST standards and guidelines are to be used for the acquisition of security technologies for the Federal Government and are not intended as restrictions on the production or use of encryption by the private sector.

5. Updates the Computer Security Act to address changes in technology over the last decade. Significant changes in the manner in which information technology is used by the Federal Government have occurred since the enactment of the Computer Security Act. The bill updates the Act, by including references to computer networking which have become an increasingly important component of the Federal Government Information technology system.

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

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

8. 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.

9. 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.

Chairman SENSENBRENNER. I ask the members to proceed with the amendments in the order on the roster.

Without objection, all members' opening statements will be placed in the record at this point.

[The opening statement and attachment of Chairman Sensenbrenner and the opening statements of Mr. Brown, Mr. Gordon, and Mr. Doyle follow:]

STATEMENT OF CHAIRMAN SENSENBRENNER

MARKUP OF H.R. 1903, THE COMPUTER SECURITY ENHANCEMENT ACT OF 1997

On June 17, 1997, I introduced H.R. 1903, the Computer Security Enhancement Act of 1997, with Ranking Member Brown, Technology Subcommittee Chairwoman Morella and Ranking Member Gordon and nine other members of the Committee. Since its introduction, an additional 13 members of the Committee have cosponsored the bill.

H.R. 1903 updates the Computer Security Act of 1987 to take into account the evolution of computer networks and their use by both the Federal Government and the private sector. The bill recognizes that the current lack of security for electronic data at federal agencies is a major national security risk. Using the National Institute of Standards and Technology (NIST), H.R. 1903 attempts to harness the power of the private sector to help improve computer security at federal civilian agencies.

In the interest of brevity, and with the knowledge that a majority of the Committee already supports the bill, I will not recapitulate all the reasons to vote for H.R. 1903. However, if you are interested, I would commend you to read the article by Congressman Brown and me which appeared in yesterday's Roll Call.

In closing, I would like to thank Congressman Brown, and the members of the Technology Subcommittee—especially Chairwoman Morella and Ranking Member Gordon—for their hard work in crafting a bill that promises to improve computer security throughout the Federal Government.

[The article referred to follows:]

Page 10 ROLL CALL Cyberpolicy Briefing Monday, July 28, 1997

Unclassified Databases Contain Enormous Amounts Of Personal Information. Let's Make Sure They're Protected.

By Rep. James Sensenbrenner and Rep. George Brown

Gone is the "small town" charm and civility of the Internet. The exponential growth of online society has brought with it many of the same problems found when a quiet hamlet becomes a thriving metropolis almost overnight.

And today the chief impediment to the continued growth of the Internet is security — the assurance that sensitive personal information can travel the Net without fear of theft, corruption, or disclosure.

No one questions whether the Internet will enhance commerce, nor does anyone question that the Internet offers individuals access to data on a scale that only five years ago was inconceivable.

In fact, the potential for commerce on the Internet seems almost unlimited. The Internet already allows businesses to buy and sell, find employees, exchange money, and organize their manufacturing and supply operations. Customers can shop for products, engage in banking, trade stocks, and make travel reservations. And the current range of services is just the beginning.

Already, world trade involving computer software, entertainment products, information services, technical information, product licenses, financial services, and professional services accounts for well more than $40 billion in exports. In the future, an increasing share of these transactions will occur online. Internet commerce was valued at $200 million in the US in 1996 and is projected to grow tenfold by 2000.

The lack of security is the greatest inhibition to the future growth of Internet commerce. For electronic commerce to reach its potential will require a reliable, secure, and trustworthy environment. To buy or sell over the network, consumers and businesses will need to have confidence that a transaction is legitimate. They will need a system where they can be sure of the integrity of the information they receive and the security of the information they send. The Internet needs to provide assurances that there will not be improper access to classified or private information.

Already, world trade involving computer software, entertainment products, information services, technical information, product licenses, financial services, and professional services accounts for well more than $40 billion in exports. In the future, an increasing share of these transactions will occur online. Internet commerce was valued at $200 million in the US in 1996 and is projected to grow tenfold by 2000.

The lack of security is the greatest inhibition to the future growth of Internet commerce. For electronic commerce to reach its potential will require a reliable, secure, and trustworthy environment. To buy or sell over the network, consumers and businesses will need to have confidence that a transaction is legitimate. They will need a system where they can be sure of the integrity of the information they receive and the security of the information they send. The Internet needs to provide assurances that there will not be improper access to classified or private information.

Already, cracks are appearing in the electronic network that may undermine public confidence in the Internet's integrity. For example, just a few weeks ago, hundreds of users of two of the most popular sport sites on the Web — ESPN SportsZone and NBA.com — received anonymous e-mail messages with the last eight digits of their credit card numbers.

And this is not an isolated incident. Almost weekly there are stories about a hacker breaking the integrity of databases via an Internet connection.

Security for sensitive data is not just a challenge for the private sector. The federal government holds extensive records on all US citizens. Just as in the private sector, the lack of adequate security for federal civilian computer systems is a significant problem. Since June 1993, the General Accounting Office has issued more than 30 reports detailing serious information-security weaknesses at federal agencies.

In a September 1996 report, the GAO reported that over the past two years serious information-control weaknesses existed at ten of the 15 largest federal agencies. The significance of these weaknesses cannot be understated. According to another GAO report, in 1995 alone, the Department of Defense may have experienced as many as 250,000 "attacks" on its computer systems. It is estimated that fully 64 percent of these attacks succeed.

Rep. James Sensenbrenner (R-Wis) is chairman of the Science Committee. Rep. George Brown (D-Calif) is the panel's ranking member.

and the Federal Aviation Administration

Both of these agencies are committed to improving public safety through the use of improved transmission of electronic data. The FAA, for example, is currently pursuing the concept of "free flight," allowing unprecedented flexibility for pilots in the air to plan and reorient their routes as new information from other planes and ground control is relayed to them through digital data transmissions.

What is surprising to us is that the current political debate over encryption has focused almost solely on the needs of law enforcement versus personal privacy. There is little discussion of the larger issue — how to make computer systems secure.

And the issue is not simply securing transient communications over the Internet, but securing databases from unwarranted, unauthorized intrusion via an Internet connection — from collections of credit card numbers to confidential business plans to individual IRS information. Once a computer system is linked to the Internet, it is vulnerable to attacks through that connection.

Government agencies, businesses, and individuals are still largely unaware that while the Internet gives them access to an electronic world, it also lets hackers into their personal world. One of the central findings of the 1996 National Research Council's (NRC) report, "Cryptography's Role in Securing the Information Society," is the relative lack of attention paid to securing electronic information. People still haven't made the leap from the concept that physically securing data or a data system (locking computer disks in filing cabinets or computer systems in buildings) provides little security in an electronic world.

If we want to reap the full extent of the government's investment in new technologies, we must ensure that the government, the business

sector, and the public have access to high-quality computer security.

Although the debate so far has centered around the twin issues of encryption and cryptography, this is only one element of a comprehensive computer security system. One of the more surprising findings of the NRC study was that many of the cryptographic products on the market don't really provide that much security. Today, consumers of cryptographic products have to rely on vendors' claims regarding the reliability of their products. There is no Good Housekeeping Seal of Approval for encryption products.

We feel that there is a strong need to encourage the development of good, reliable encryption products in the commercial market to foster the growth of the electronic telecommunications network America has created.

Working with technology subcommittee Chairwoman Morella and ranking member Bart Gordon (D-Tenn), we developed legislation — H.R. 1903, the Computer Security Enhancement Act of 1997 — with the objective of enhancing the security of non-classified government information by promoting the development of reliable encryption products by the commercial sector and requiring their use by federal agencies whenever possible.

H.R. 1903, which the Science Committee will markup tomorrow, departs from past practices of instituting separate security standards for government. The legislation explicitly requires the National Institute of Standards and Technology (NIST) to develop evaluation and testing procedures for commercially available security products and to actively promote the use by federal agencies of off-the-shelf technologies to meet their computer and network security requirements. This in turn will support the growth of electronic commerce.

H.R. 1903 builds on the close collaboration between NIST and industry in developing standards. H.R. 1903 strengthens NIST's role in coordinating federal agencies' efforts to utilize encryption and digital identification products. In addition, this legislation allows NIST to evaluate the technical merit of industry claims of the strength of generally available foreign encryption products. Among other benefits, this provision should help defuse some of the tension surrounding the issue of exporting domestic encryption products.

The most important underlying element of H.R. 1903 is that it recognizes that the security needs of the government and the private sector are similar. Hopefully, the result will be lower cost and better security for everyone.

The electronic transmission of data has been with us since the advent of the telegraph. The potential for falsifying, stealing, or corrupting it is not new. Fax transmissions are no more secure than the phone lines and airways over which they travel, and we all know that cell phone conversations are often less than private. What has changed, however, is the volume of data we now transmit and store electronically.

Ultimately, the Internet's own success is providing its greatest challenge. Just as escalating rates of crime in growing urban centers will slow, and in some cases reverse, a city's economic boom, the lack of security on the Internet will have significant consequences for the commercial viability of the system.

The democratization of the Internet has the potential to yield tremendous benefits to our nation's economy. In order to sustain this tremendous rate of growth, more attention must be paid to the Net's security. The federal government in particular must do more to ensure that the electronic data it stores and transmits is protected. H.R. 1903 is an important step in that direction.

STATEMENT OF HON. GEORGE E. BROWN, JR.

Mr. Chairman, I am pleased to have joined you as an original cosponsor of H.R. 1903, the Computer Security Enhancement Act of 1997, and applaud you for bringing the bill expeditiously before the Committee for its consideration.

H.R 1903 was developed as a collaborative initiative by Majority and Minority members of the Science Committee. In particular, I would like to acknowledge the valuable contributions of Mrs. Morella, the Technology Subcommittee Chairwoman, and Mr. Gordon, the Ranking Democratic Member of the Subcommittee, in crafting the bill and in working together to report it from the Technology Subcommittee.

I will defer to Mrs. Morella and to Mr. Gordon for an explanation of the provisions of H.R. 1903, but will say a few words about the intent of the legislation.

A decade ago, the Committee was instrumental in the passage of a measure that gave NIST the responsibility for the protection of unclassified information in federal computer systems. The Computer Security Act of 1987 charged NIST to develop appropriate technical standards and administrative guidelines, as well as guidelines for training federal employees in security practices.

Overall, NIST has received mixed reviews on its performance in carrying out its responsibilities under the 1987 statute. The agency has been criticized for allowing the National Security Agency to exercise too much influence on the development of standards for unclassified federal computer systems, and for developing standards that were inconsistent with emerging market standards. Also, according to NIST's external advisory committee, more effort should be devoted to providing advice and assistance to federal agencies in meeting their information security needs.

H.R. 1903 seeks to elevate NIST's commitment to meeting its responsibilities under the Computer Security Act. It also reinforces that NIST has the primary responsibility for the protection of unclassified federal computer systems and networks.

Two main themes of the bill are to expand the use of validated, commercially available cryptography technologies and to ensure greater public input into the development of standards and guidelines for federal systems.

The threats to electronic information are much greater than when the 1987 legislation was considered by the Committee. H.R. 1903 is an important step toward addressing this vulnerability. I encourage my colleagues to support reporting the bill from Committee.

STATEMENT OF HON. BART GORDON

Chairman Sensenbrenner has explained the provisions of H.R. 1903 and many of us are co-sponsors of this legislation. Therefore, I will keep my statement very brief.

I want to highlight the underlying purpose of this legislation—to encourage the use of encryption products, both by the Federal Government and the private sector. I am convinced that we must have a trustworthy and secure electronic network system to foster the growth of electronic commerce. This bill builds on the successful track record of the National Institute of Standards and Technology in working with industry and other federal agencies to develop a consensus on the necessary standards and protocols required for electronic commerce.

The Technology Subcommittee marked-up this bill yesterday and approved two amendments which strengthen H.R. 1903. Chair Morella has mentioned her amendment and I would like to take a few moments to explain the provisions that I added to this legislation.

First: they increase public awareness of the need to improve the security of communication networks by requiring the Technology Administration to establish a clearinghouse of public information on electronic security threats; and

Second: they establish a coordination mechanism in the development of a national digital signature infrastructure by establishing a national panel of federal, state, business, technical and legal experts.

Digital signature technology is essential to ensure public trust of networks such as the Internet. Digital signature verifies that the business or individual you are communicating with is who you think they are and that the information being exchanged has not been altered in transit.

For this technology to be deployed, a trusted guarantor of the digital signature must exist—a certification authority. Several States already have statutes in place to regulate this technology. However, for a national system to develop uniform standards must be in place. Without this national uniformity, variations will exist among different state requirements for certification authorities which could affect the reliability and security of the operations associated with issuing and managing certificates.

These provisions do not give the Federal Government the authority to establish standards or procedures. We simply create a national panel of public and private representatives to begin to address how to develop and integrate a national policy regarding digital signatures.

This legislation is consistent with recommendations of the Office of Technology Assessment, the National Research Councils and independent experts who have appeared before the Subcommittee.

Finally, the underlying principle of H.R. 1903 is that it recognizes that government and the private sector security needs are similar. Hopefully the result will be lower cost and better security for everyone.

This bill is the result of bipartisan cooperation and it has been a pleasure working with Chair Morella on this issue. I urge my colleagues to support this legislation.

STATEMENT OF HON. MIKE DOYLE (PA–18)

I am pleased that the Committee on Science is moving forward with H.R. 1903, the Computer Security Enhancement Act, of which I am a cosponsor.

As our society becomes more and more reliant on information technology, it is imperative that public policy keep pace with technological advancement. This is quite a challenge for a deliberative body like Congress, given the phrenetic pace with which information-related advancements have occurred.

In Pittsburgh, we are quite proud of the Software Engineering Institute, which has been—and continues to be—a global leader in bringing together encryption capability and encryption policy. I have drawn on their expertise often throughout my service on the Science Committee, and I would encourage the Committee to look towards SKI as a resource in any future considerations on this or related issues.

Through the extensive hearings held by the Technology Subcommittee, we have identified that the basic encryption needs of government and the private sector are quite similar. Furthermore, recent events have demonstrated that encryption methods currently billed as intelligent solutions to these problems are inadequate and inconsistent. This legislation is the first effort to engage the Federal Government in certifying the effectiveness and consistency in the setting of encryption standards.

The Computer Security Enhancement Act is measured approach to the issues that are within the Committee on Science's jurisdiction. I want to express my appreciation to Chairman Sensenbrenner for introducing this legislation, and to the Technology Subcommittee Chairwoman Morella and Ranking Member Bart Gordon for making sure that the concerns of all members were addressed. I must also express my regard for George Brown, the Ranking Member of the Full Committee, who has been working on this issue for many years and whose wisdom is evident throughout this legislation.

Chairman SENSENBRENNER. The gentlewoman from Maryland, Mrs. Morella, has an amendment and is recognized for 5 minutes.

Without objection the amendment is considered as read and open for amendment at any point.

[The Amendment Roster and the text of the amendment follow:]

COMMITTEE ON SCIENCE

FULL COMMITTEE MARKUP

July 29, 1997

AMENDMENT ROSTER

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

No.	Sponsor	Description	Results
1.	Mrs. Morella and Mr. Gordon	H.R. 1903, as reported by the Subcommittee on Technology on July 28, 1997	

H.R. 1903, AS REPORTED BY THE SUBCOMMITTEE ON TECHNOLOGY ON JULY 28, 1997

Strike all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Security Enhancement Act of 1997".

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.

(5) Federal policy for control of the export of encryption technologies should be determined in light of the public availability of comparable encryption technologies outside of the United States in order to avoid harming the competitiveness of United States computer hardware and software companies.

(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;

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

(3) provide the assessment of the capabilities of information security products incorporating cryptography that are generally available outside the United States.

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 (f) and (g), 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 of Commerce in accordance with subsection (a)(4). No standards or guidelines shall be submitted to the Secretary prior to the receipt by the Institute of the Board's written recommendations. The recommendations of the Board shall accompany standards and guidelines submitted to the Secretary.

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

SEC. 7. EVALUATION OF CAPABILITIES OF FOREIGN ENCRYPTION.

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 (d), as added by section 6 of this Act, the following new subsection:

"(e)(1) If the Secretary has imposed, or proposes to impose, export restrictions on a product that incorporates encryption technologies, the Institute may accept technical evidence from the commercial provider of the product offered to indicate that encryption technologies, embodied in the form of software or hardware, that are offered and generally available outside the United States for use, sale, license, or transfer (whether for consideration or not) provide stronger participation for privacy of computer data

and transmissions of information in digital form than the encryption technologies incorporated in the commercial provider's product.

"(2) Within 30 days after accepting technical evidence from a commercial provider under paragraph (1), the Institute shall evaluate the accuracy and completeness of the technical evidence and transmit to the Secretary, and to the Committee on Science of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate, a report containing the results of that evaluation. The Institute may obtain assistance from other Federal and private sector entities in carrying out evaluations under this paragraph.

"(3) Not later than 180 days after the date of the enactment of the Computer Security Enhancement Act of 1997, the Institute shall develop standard procedures and tests for determining the capabilities of encryption technologies, and shall provide information regarding those procedures and tests to the public.

"(4) The Institute may require a commercial provider seeking evaluation under this subsection to follow procedures and carry out tests developed by the Institute pursuant to paragraph (3).".

SEC. 8. 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:

"(h) 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. 9. 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 (f), 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 (f)(2), as so redesignated by section 5(1) of this Act, by striking "(b)(5)" and inserting in lieu thereof "(b)(5)"; and

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

SEC. 10. 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. 11. COMPUTER SECURITY FELLOWSHIP PROGRAM.

There are authorized to be appropriated to the Secretary of Commerce $250,000 for fiscal year 1998 and $500,000 for fiscal year 1999 for the Director of the National Institute of Standards and Technology for fellow-

ships, 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. 12. 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 Com-

merce $450,000 for fiscal year 1998, to remain available until expended, for carrying out this section.

SEC. 13. 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. 14. DIGITAL SIGNATURE INFRASTRUCTURE.

(a) NATIONAL POLICY PANEL.—The Under Secretary of Commerce for Technology shall establish a National Policy Panel for Digital Signatures. The Panel shall be composed of nongovernment and government technical and legal experts on the implementation of digital signature technologies, individuals from companies offering dig-

ital signature products and services, State officials, including officials from States which have enacted statutes establishing digital signature infrastructures, and representative individuals from the interested public.

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

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

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

(3) audit standards for certification authorities.

(c) ADMINISTRATIVE SUPPORT.—The Under Secretary of Commerce for Technology shall provide administrative support to the Panel established under subsection (a) of this section as necessary to enable the Panel to carry out its responsibilities.

SEC. 15. SOURCE OF AUTHORIZATIONS.

Amounts authorized to be appropriated by this Act shall be derived from amounts authorized under the Na-

tional Institute of Standards and Technology Authorization Act of 1997.

Mrs. MORELLA. Thank you, Mr. Chairman.

I want to thank all of the members who have aided in the support of the Computer Security Enhancement Act. Yesterday the Technology Subcommittee, which I chair, reported H.R. 1903 by unanimous voice vote. Further, the bill currently has over half of the Full Committee as co-sponsors.

What the bill does is it promotes the maximum protection of our federal civilian agency computer system while also supporting American companies.

By encouraging the use of commercially available computer security products, H.R. 1903 takes advantage of the wealth of commercial expertise on securing information networks.

It also provides for a wealth of new information-sharing between NIST and the private sector which should aid businesses and federal agencies in safeguarding their sensitive electronic information.

Most importantly, H.R. 1903 emphasizes the need for strong security. The widespread use of strong encryption will promote safety, security, and privacy. So I encourage my colleagues to support it in our markup.

I would defer to Mr. Gordon for any comments he may like to make on behalf of the amendment.

Chairman SENSENBRENNER. The gentleman from Tennessee.

Mr. GORDON. Thank you, Mr. Chairman.

Following the spirit of your earlier request, I will submit my statement for the record and just thank Chairwoman Morella for the courtesies. It was good to work with her on this bill.

This is a good bill. It passed unanimously in our Subcommittee yesterday.

Mr. Chairman, I invite you to join us today in celebrating the continuation of the deficit reduction package that was passed in 1993 with 100 percent of support from Democrats and no help from the Republicans. So we hope now that, since that has proven to be a success, that, as John Kasich said, if it was successful he would become a Democrat, we hope that he will join us, and you are welcome to join us also. [Laughter.]

Chairman SENSENBRENNER. Well, if the gentleman would yield, there is a big difference. The deficit reduction package increased taxes. The Balanced Budget Act decreases taxes, and that is what is bringing all the Republicans on board.

The question is on the amendment in the nature of a substitute offered by the gentlewoman from Maryland, Mrs. Morella, and the gentleman from Tennessee, Mr. Gordon.

Is there any further discussion?

[No response.]

Chairman SENSENBRENNER. Hearing none, all those in favor will signify by saying, aye.

[Chorus of ayes.]

Chairman SENSENBRENNER. Opposed, no?

[No response.]

Chairman SENSENBRENNER. The ayes have it.

Are there any further amendments?

[No response.]

Chairman SENSENBRENNER. There are no further amendments.

The Chair recognizes the gentleman from Tennessee for a motion.

Mr. GORDON. Mr. Chairman, I move the Committee report the bill, H.R. 1903, the Computer Security Enhancement Act of 1997, As amended.

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

Chairman SENSENBRENNER. The question is on the motion to report the bill favorably. The Chair notes the presence of a reporting quorum.

All those in favor will signify by saying, aye.

[Chorus of ayes.]

Chairman SENSENBRENNER. Opposed, no?

[No response.]

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

Without objection, the Motion to Reconsider is laid upon the table.

[No response.]

Chairman SENSENBRENNER. Without objection, all members will have 2 subsequent calendar days in which to submit Supplemental, Minority or Additional views on the measure.

[No response.]

Chairman SENSENBRENNER. Without objection, pursuant to Clause 1 of Rule 20 of the Rules of the House of Representatives, 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.

Is there objection to any of these unanimous consent requests?

[No response.]

Chairman SENSENBRENNER. Hearing none, so ordered.

[Whereupon, at 1:18 p.m., the markup of H.R. 1903 was completed and the Committee immediately proceeded to consideration of H.R. 2249.]

○