HEINONLINE

Citation: 4 Bernard D. Reams Jr. Law of E-SIGN A Legislative
of the Electronic Signatures in Global and National
Act Public Law No. 106-229 2000 H7293 2002

Content downloaded/printed from
HeinOnline (http://heinonline.org)
Sun Apr 21 21:29:18 2013

-- Your use of this HeinOnline PDF indicates your acceptance
of HeinOnline's Terms and Conditions of the license
agreement available at http://heinonline.org/HOL/License

-- The search text of this PDF is generated from
uncorrected OCR text.

his humor and warmth and for his commitment to our country. He was a great war hero and did so much for the USO. All that and he played a mean game of golf. I'm going to miss him."

Bob's wife Dolores said, "His life was lonely without his beloved wife Gloria, who died in 1994. He missed her so, and now they're together again. What joy there must be."

"It's A Wonderful Life" and "Mr. Smith Goes To Washington" are stories of commitment to principle and to family. These movies are a far cry from many of the movies we see today, characterized by "Powder", "Pulp Fiction" and "Priest."

We need to continue to send Hollywood the message that America longs for movies in the spirit of Jimmy Stewart, movies about commitment to family, to a husband or a wife, commitment to children, to love them and care for them, to put them first, not our own selfish interests.

Again, I commend the gentleman from New York for bringing forward this legislation, and the subcommittee chairman and the ranking member for supporting it.

Mr. MICA. Mr. Speaker, I yield myself the balance of our time.

Mr. Speaker, I want to take a moment to thank again the distinguished gentleman from New York [Mr. KING] for bringing this resolution before the House. I also want to take a moment to thank the distinguished gentleman from Pennsylvania [Mr. MURTHA] for his leadership relating to this memorial to a great American, and the gentleman from Maryland [Mr. CUMMINGS], my colleague and distinguished ranking member of our Subcommittee on Civil Service, for his assistance in bringing this resolution to the floor.

□ 1300

Of course, I also want to thank Chairman BURTON, chairman of our full committee, and the ranking member, the gentleman from California [Mr. WAXMAN], who has also helped in expediting the consideration of this resolution.

In closing, Mr. Speaker, I thought it would be interesting to read from "Mr. Smith Goes to Washington," a 1939 classic about Congress, and Mr. Stewart's famous words as Mr. Smith. He said, as many of us remember, about his feelings, "I wouldn't give you two cents for all your fancy rules if behind them they didn't have a little bit of plain, ordinary kindness and a little lookin' out for the other fella." And that is what Congress is sometimes about, and we remember that as we remember this great American today.

Mr. Speaker, as we have heard on the floor today, Jimmy Stewart was an exemplary American. He personified the traditional American virtues of hard work, dedication to family, dedication to country, and personal modesty. He enriched our culture, and he enriched our civic life.

He could have used his heroic military service during World War II to bring additional glory to himself, but like so many of the men and women of his era who served our Nation in war at a perilous time, he did not. Instead, he served his Nation quietly. I have read, Mr. Speaker, that Jimmy Stewart only once used his influence while in the military. He used it to request that he be treated the same as all other men and women in uniform.

It is indeed a privilege for me, Mr. Speaker, to join my distinguished colleague, the gentleman from New York [Mr. KING], and all Members to support this resolution, recognizing the many and lasting contributions of James Maitland Stewart.

The SPEAKER pro tempore (Mr. LAHOOD). The question is on the motion offered by the gentleman from Florida [Mr. MICA] that the House suspend the rules and agree to the concurrent resolution, House Concurrent Resolution 109.

The question was taken.

Mr. CONDIT. Mr. Speaker, I object to the vote on the ground that a quorum is not present and make the point of order that a quorum is not present.

The SPEAKER pro tempore. Pursuant to clause 5 of rule I and the Chair's prior announcement, further proceedings on this motion will be postponed.

The point of no quorum is considered withdrawn.

GENERAL LEAVE

Mr. MICA. Mr. Speaker, I ask unanimous consent that following passage of this legislation, all Members may have 5 legislative days within which to revise and extend their remarks on the concurrent resolution, House Concurrent Resolution 109.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Florida?

There was no objection.

MESSAGE FROM THE PRESIDENT

A message in writing from the President of the United States was communicated to the House by Mr. Sherman Williams, one of his secretaries.

COMPUTER SECURITY ENHANCEMENT ACT OF 1997

Mr. SENSENBRENNER. Mr. Speaker, I move to suspend the rules and pass 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, as amended.

The Clerk read as follows:

H.R. 1903

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;".

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) H7293 2002

SEC. 5. COMPUTER SECURITY IMPLEMENTATION.

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

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

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

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

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

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

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

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

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3), as amended by this Act, is further amended by inserting after subsection (c), as added by section 5 of this Act, the following new subsection:

"(d)(1) The Institute shall solicit the recommendations of the Computer System Security and Privacy Advisory Board, established by section 21, regarding standards and guidelines that are being considered for submittal to the Secretary 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. LIMITATION ON PARTICIPATION IN REQUIRING ENCRYPTION STANDARDS.

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

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

SEC. 8. MISCELLANEOUS AMENDMENTS.

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

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

(2) in subsection (e), as so redesignated by section 5(1) of this Act, by striking "shall draw upon" and inserting in lieu thereof "may draw upon";

(3) in subsection (e)(2), as so redesignated by section 5(1) of this Act, by striking "(b)(5)" and inserting in lieu thereof "(b)(8)"; and

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

SEC. 9. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.

Section 5(b) of the Computer Security Act of 1987 (49 U.S.C. 759 note) is amended—

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

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

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

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

SEC. 10. COMPUTER SECURITY FELLOWSHIP PROGRAM.

There are authorized to be appropriated to the Secretary of Commerce $250,000 for fiscal year 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. 11. STUDY OF PUBLIC KEY INFRASTRUCTURE BY THE NATIONAL RESEARCH COUNCIL.

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

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

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

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

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

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

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

(c) INTERAGENCY COOPERATION WITH STUDY.—All agencies of the Federal Government shall cooperate fully with the National Research Council in its activities in carrying out the study under this section, including access by properly cleared individuals to classified information if necessary.

(d) REPORT.—Not later than 18 months after the date of the enactment of this Act, the Secretary of Commerce shall transmit to the Committee on Science of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report setting forth the findings, conclusions, and recommendations of the National Research Council for public policy related to public key infrastructures for use by individuals, businesses, and government. Such report shall be submitted in unclassified form.

(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary of Commerce $450,000 for fiscal year 1998, to remain available until expended, for carrying out this section.

SEC. 12. PROMOTION OF NATIONAL INFORMATION SECURITY.

The Under Secretary of Commerce for Technology shall—

(1) promote the more widespread use of applications of cryptography and associated technologies to enhance the security of the Nation's information infrastructure;

(2) establish a central clearinghouse for the collection by the Federal Government and dissemination to the public of information to promote awareness of information security threats; and

(3) promote the development of the national, standards-based infrastructure needed to support commercial and private uses of encryption technologies for confidentiality and authentication.

SEC. 13. 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. 14. 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.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Wisconsin [Mr. SENSENBRENNER] and the gentleman from Tennessee [Mr. GORDON] each will control 20 minutes.

The Chair recognizes the gentleman from Wisconsin [Mr. SENSENBRENNER.]

Mr. SENSENBRENNER. Mr. Speaker, today, in a bipartisan effort, the Committee on Science brings to the floor H.R. 1903, the Computer Security Enhancement Act of 1997. I would like to thank the ranking member, the gentleman from California, Mr. GEORGE BROWN, the Subcommittee on Technology chairwoman, the gentlewoman from Maryland, Mrs. CONSTANCE MORELLA, the ranking member of the subcommittee, the gentleman from

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) H7294 2002

Tennessee Mr. BART GORDON, as well as the 25 other members of the committee who cosponsored this bill.

The Computer Security Act of 1987 gave authority over computer and communication security standards in Federal civilian agencies to the National Institute of Standards and Technology. The Computer Security Enhancement Act of 1997 strengthens that authority and directs funds to implement practices and procedures which will ensure that the Federal standard-setting process remains strong, despite its increasing reliance on a network infrastructure.

The need for this renewed emphasis on the security of Federal civilian agencies is underscored by a recently released report from the General Accounting Office. The 1997 Report on Information Management and Technology highlighted information security as a Governmentwide high-risk issue. It stated that despite having critical functions, Federal systems and data are not adequately protected.

Since June 1993, the GAO has issued over 30 reports describing serious information security weaknesses at Federal agencies. In September 1996, it reported that during the previous 2 years, such weaknesses had been determined for 10 of the 15 largest Federal agencies. For half of these agencies, the weakness had been disclosed repeatedly for 5 years or longer.

Much has changed in the 10 years since the Computer Security Act of 1987 became law. The proliferation of network 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 buying decisions for computer security hardware on NIST standards.

Specifically, H.R. 1903 requires NIST to encourage the acquisition of off-the-shelf products to meet civilian agencies' security needs. Such practices will reduce the cost and improve the availability of computer security technologies for Federal civilian agencies.

The bill strengthens the role played by the independent Computer System Security and Privacy Advisory Board in NIST's decision-making process. The CSSPAB, which is made up of representatives from industry, Federal agencies, and private organizations, has long been considered a vital part of NIST's standard-setting process on emerging computer security issues. Strengthening the board's role will help ensure that the Federal Government benefits from private sector expertise.

H.R. 1903 establishes a new computer science fellowship program for graduate and undergraduate students studying computer security.

It provides for the National Research Council to study the desirability of key infrastructures. The NRC would also examine the technologies required for establishing such an infrastructure.

Further, the bill requires the Under Secretary of Commerce for Technology to actively promote the use of technologies that will enhance the security of communications networks and electronic information; to establish a clearinghouse of information available to the public on information security threats; and to promote the development of standards-based infrastructure that will enable the widespread use of encryption technologies for confidentiality and authentication.

Finally, H.R. 1903 establishes a national panel to discuss digital signatures. The panel will explore all factors associated with developing a national digital signature infrastructure based on uniform standards.

Mr. Speaker, Members will notice the old section 7 directing NIST to assess foreign encryption products has been removed, to satisfy the concerns of the administration and my colleagues on the Permanent Select Committee on Intelligence. I trust this action will help assure that all Members can support this legislation without reservation.

Mr. Speaker, the Computer Security Enhancement Act of 1997 will ensure that Federal civilian agencies enjoy the highest standard of information technologies, both for transmitted and stored data. The protection of this vital data is necessary for the security of all Americans.

Mr. Speaker, I encourage my colleagues to support this measure, and I reserve the balance of my time.

Mr. GORDON. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in strong support of H.R. 1903, the Computer Security Enhancement Act of 1997. I am an original cosponsor of H.R. 1903, and have worked closely with the chairman, the gentlewoman from Maryland [Mrs. MORELLA], to improve the bill during the Subcommittee on Technology's deliberations.

Not a day goes by that we do not see some reference to the Internet and the explosive growth of electronic commerce. What was originally envisioned as a network of defense communications and university researchers has now become an international communications network, of which we are just beginning to realize its potential.

Reports from both the Office of Technology Assessment and the National Research Council have identified a major obstacle to the growth of electronic commerce: the lack of widespread use of computer security products. H.R. 1903 is a first step to encourage the use of computer security products, both by Federal agencies and the private sector, which in turn will support the growth of electronic commerce.

I want to highlight the underlying purpose of this legislation: to encourage the use of computer security products, both by Federal agencies 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.

H.R. 1903 builds upon 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 would like to take a few minutes to explain provisions I added to this legislation. One of the provisions aims to increase the 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 the other provision I felt necessary was to establish a coordination mechanism in the development of national digital signature infrastructure by establishing a national panel of business, technical, legal, State, and Federal experts.

Digital signature technology is essential to ensure the public trust of networks such as the Internet. Digital signature verifies that the businesses or individual we are communicating with is who we think they are, and that the information being exchanged has not been altered in transit. For this technology to be developed, a trusted certification authority for the digital signature must exist.

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 uniformity, variations will exist among different State requirements for certification authorities which could affect the reliability and security of operations associated with issuing and managing certification.

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 consistent policy regarding digital signatures.

H.R. 1903 is entirely consistent with recommendations of the Office of Technology Assessment, the National Research Council, and independent experts who have appeared before the subcommittee. I want to stress that the underlying principle of H.R. 1903 is that it recognizes that Government and private sector computer security needs are similar. Hopefully the result will be lower cost and better security for everyone.

This bill is a result of bipartisan cooperation. It has been a pleasure working with Chairman MORELLA on this legislation, as well as Chairman SENSENBRENNER and the former chairman, the gentleman from California, [Mr. GEORGE BROWN]. I urge my colleagues to support H.R. 1903.

Mr. Speaker, I reserve the balance of my time.

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) H7295 2002

Mr. SENSENBRENNER. Mr. Speaker, I yield 2 minutes to the gentleman from Virginia [Mr. DAVIS].

Mr. DAVIS of Virginia. Mr. Speaker, I appreciate the chairman yielding time to me.

Mr. Speaker, I very enthusiastically support H.R. 1903, the Computer Security Enhancement Act. This amends, of course, the 1987 act, because the world has changed since 1987. Last year the Department of Defense systems experienced as many as 250,000 attacks, just in 1995. It was estimated that 64 percent of these attacks were successful in gaining access to the Department of Defense systems. I think Federal agencies have to employ appropriate countermeasures, and today we are not set to do that.

With the growth in the Internet, individual users across the country are relying more and more and on communications and business commerce through the Internet, but the testimony before the committee shows that there continue to be problems, and the technologies to better protect users does not exist. Security problems in individual computers that connect to the Internet are very much at risk.

One interesting note, and I think this starts to address it with a system that authorizes the National Institute of Standards to reserve $750,000 for new computer science fellowship programs for students to study security. Of 5,500 Ph.D.'s granted in computer science and engineering last year, a scant 16 pertained to computer security. It is not even a required course to get a doctorate in computer science and engineering. Only 50 percent of the 16 were given to U.S. nationals.

Mr. Speaker, I think this will start to move in a different direction and rectify this. I congratulate the chairman of the committee, the ranking member, and others who are cosponsoring this. I think it is a needed change. I rise in support, and ask my colleagues to support it.

Mr. GORDON. Mr. Speaker, I yield 5 minutes to the gentleman from California [Mr. BROWN], my leader and mentor on the Committee on Science.

(Mr. BROWN of California asked and was given permission to revise and extend his remarks.)

Mr. BROWN of California. Mr. Speaker, I thank the gentleman for yielding time to me. I appreciate the opportunity to speak briefly on this subject.

Mr. Speaker, I recognize that the gentleman has already, together with the chairman, the gentleman from Wisconsin [Mr. SENSENBRENNER], laid out the basic content of the legislation, and I hope I do not duplicate what he has said unnecessarily.

□ 1315

I am, of course, in support of H.R. 1903, the Computer Security Enhancement Act of 1997. This bill will increase the protection of electronic information in Federal computer systems, and moreover, will help to stimulate the development of computer hardware and software technologies by American companies.

The bill was developed as a collaborative initiative by majority and minority members of the Committee on Science, and I applaud the efforts of the gentleman from Wisconsin [Mr. SENSENBRENNER], the chairman, in moving the bill expeditiously through the committee and bringing it to the floor as he has on so many other bills before our committee.

I would also like to acknowledge the valuable contribution of the gentlewoman from Maryland [Mrs. MORELLA], the chair of the Subcommittee on Technology, and the gentleman from Tennessee [Mr. GORDON], the ranking Democratic member of the subcommittee, who I am sure all of my colleagues recognize actually do the difficult work of developing the language in legislation of this sort and making whatever necessary compromises have to be made. I of course will defer to their judgment as to what needs to be in a bill of this sort.

A decade ago the Committee on Science was instrumental in the passage of a measure that gave the National Institute of Standards and Technology the responsibility for the protection of unclassified information in Federal computer systems. Specifically, 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. We were just beginning to recognize at that time the importance of these new technology communication initiatives which are becoming such an important part of our lives today.

Overall, NIST has received somewhat 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.

We in California, of course, are very much concerned with the role we play in global commerce in systems of this sort because such a large part of new developments in this area occur in California and it has become a large part of our economy.

Also, according to NIST's external advisory committee, the agency ought to devote greater resources and effort to providing advice and assistance to Federal agencies in order to help them to satisfy 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 the policy established by the 1987 act that NIST has the primary responsibility for the protection of unclassified Federal computer systems and networks.

Mr. Speaker, I want to emphasize two important themes of the bill. First, it seeks to expand the use of validated commercially available cryptography technologies by Federal agencies, which will in turn stimulate the U.S. market for computer security products; and, second, the bill puts in place mechanisms to ensure greater public participation in the development of computer security standards and guidelines for Federal systems.

The threats to electronic information are much greater than when the Computer Security Act was passed in the House in 1987. H.R. 1903 is an important step toward addressing this vulnerability.

Mr. Speaker, I commend H.R. 1903 to my colleagues for their approval and encourage their support for its passage in the House.

Mrs. MORELLA. Mr. Speaker, I rise in support of H.R. 1903, legislation I introduced with Chairman SENSENBRENNER and ranking Members GORDON and BROWN on June 17, 1997, and which was unanimously reported out of the Technology Subcommittee, which I chair, on July 29, 1997.

The Computer Security Enhancement Act of 1997, 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.

H.R. 1903 recognizes that the U.S. Government is not grappling with the issues of data security in a vacuum. The bill encourages the setting of standards which are commercially available, thus aiding our software and hardware industries as well as assuring that the government can secure its information technology infrastructure with the most effective and cost efficient products. This is significant both because of the vital role the information infrastructure plays in our lives and the role that technology has in our economy.

Information technology security, or rather the lack of attention paid to it by the Federal Government, may well make the year 2000 computer problem seem small in comparison if we do not focus our attention on this vital area.

In their May 1996 report, the General Accounting Office [GAO] stated that the Department of Defense systems may have experienced as many as 250,000 attacks during 1995, of that total, about 64 percent of attacks were successful at gaining access to the DOD system. This information is even more troubling when you realize, as the report points out, that these numbers may be underestimated because only a small percentage of attacks are detected.

Federal agencies are incurring significant risk by not effectively employing cryptographic countermeasures for transmitted and stored data.

H.R. 1903, which seeks to promote the effective use of cryptography along with other security tools by Government agencies, is consistent with the conclusions of the National Research Council's CRISIS report and should help to ensure that Federal systems remain safe and the integrity of sensitive and private data is not compromised.

Additionally, according to statistics from the Business Software Alliance, the software industry alone is reported to have employed

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) H7296 2002

over 619,400 people last year, with an additional 1,445,600 jobs created in related industries. Placing a renewed emphasis on setting standards for procurement by Federal civilian agencies—standards which consider market driven specifications—will assist industry as well as ensure that Federal civilian agencies benefit from the wealth of knowledge which the private sector can provide.

Mr. Speaker, H.R. 1903 is a good and much needed bill. It was authored and is supported in equal measure on both sides of the aisle and carries over half of the full roster of the Science Committee as its cosponsors. I urge all my colleagues to support its passage.

Mr. TAUZIN. Mr. Speaker, I rise today to explore the issues presented by H.R. 1903, the Computer Security Enhancement Act of 1997, some of which are within the jurisdiction of the Committee on Commerce. The main purpose of H.R. 1903 appears to be to update the Computer Security Act of 1987 to improve computer security for Federal civilian agencies. This is a laudable goal. However, certain provisions of the bill before us today are not limited to issues within the purview of the National Institute of Standards and Technology [NIST], or to the improvement of computer security for Federal civilian agencies. Therefore, I must make note of the fact that the House Committee on Commerce maintains a strong jurisdictional interest in the telecommunications and commerce issues addressed in H.R. 1903.

For example, the findings listed in section 2 of H.R. 1903 include language asserting that the development and use of encryption should not be driven by Government requirements, and that export policy should be determined in light of the public availability of comparable encryption products outside the United States. Neither of these findings, nor policies to promote the findings, are within the scope of the Computer Security Act of 1987, or the authority of NIST.

Several provisions of H.R. 1903 address the use and development of a public key management infrastructure. Public key management infrastructure is an issue between private entities and law enforcement officials. Such infrastructure does not currently exist and is not part of the administrative question of how to improve computer security for Federal civilian agencies.

In addition, H.R. 1903 calls for the establishment of a national panel on digital signatures. While the formation of a panel may or my not be the right course of action, the issue is a question of electronic commerce that is completely outside the scope of this legislation.

Finally, H.R. 1903, as reported by the Committee on Science, included language that would have transferred authority currently vested in the Bureau of Export Administration to NIST. I understand this language regarding the determination of whether a product is generally available abroad has been removed from the bill before us today. However, the existence of the provision illustrates how far afield from the issue of computer security for Federal civilian agencies H.R. 1903 has traveled.

I will not plow through a provision-by-provision analysis of H.R. 1903 in my statement today. For the record, however, I must point out that H.R. 1903 seeks to establish encryption, telecommunications, and commerce policy far beyond the reach of the authority of either NIST or the Computer Security Act of 1987.

Ms. JACKSON-LEE of Texas. Mr. Speaker, I would like to thank Chairman SENSENBRENNER and Ranking Member BROWN for their work in bringing this opportunity to the House to construct a legislative response to the growing dependency of this Government and the public on computers and related technology.

As a cosponsor of this bill I would also like to thank Congresswoman MORELLA for her critical leadership in this area as chair of the Technology Subcommittee.

While telecomputing technologies have generated a great deal of excitement in our country these communications innovations have also presented daunting challenges to privacy and security both in the Federal Government and private sectors.

The challenge for this Congress is to solve the problems of security and privacy while allowing full public access and utilization of the technology to heighten the exchange of information between Government agencies and its citizens Federal computers must be secured from unwanted intrusions.

I support strong encryption products being made available to the private sector domestically and internationally to insure privacy of communications, business transactions, commercial exchanges and for the protection of Internet accessible copyrighted materials. I believe that well-thought-out Federal encryption policy is the first of many steps that this Congress can take to facilitate the development of telecomputing technology and the strengthening of domestic computer-related industries.

It concerns me that many communications today are carried over channels that are easily tapped. For example, satellites, cellular telephones, and local area networks are vulnerable to interception. Tapping wireless channels is almost impossible to detect and to stop, and tapping local area networks may be very hard to detect or stop as well.

Approximately 10 billion words of information in computer-readable form can be scanned for $1.00 today, allowing intruders, the malicious individuals or groups, or spies to gain access to sensitive information. A skilled person with criminal intentions can easily develop a program that recognizes and records all credit card numbers in a stream of unencrypted data traffic.

As a member of the House Committee on the JucicIary, I am particularly interested in the vulnerabilities and weaknesses that have been raised during hearings on government computer security on the House and Senate. Beginning last year under the direction of then Senator Nunn hearings on Security in Cyberspace were held. it is unprecedented in our Nation's history of technology dissemination that in 5 years the number of Internet users has grown from 1 million to 58 million with an estimated growth rate of 183 percent per year.

This rapid growth, which is creating the interconnection of civilian, Government, private, and foreign computers, is the foundation of the Global Information Infrastructure. The expansion of computer telecommunication technology has created growing efficiencies in information management, the delivery of goods and access to ideas. While accomplishing this end, it has created more vulnerability in networked systems that have not incorporated security measures, both private and government.

Unfortunately, as the hearings have so effectively pointed out, our Nation's information infrastructure is increasingly vulnerable to computer attack from foreign states, subnational groups, criminals and vandals. Your own staff's research revealed that computer hackers use different routes of attack, often crossing national boundaries and using private and public computer network systems. I recognize the complex and novel legal and jurisdictional issues that hinder the detection of and response to computer intrusions. However, I am equally mindful of the need to protect government systems with technology which is available from the growing problem of unwanted intrusion or tampering.

It is estimated that the private sector experiences $800 million in losses in a year according to a group of security firms who responded to an inquiry for evidence during the Senate's review of security in cyberspace.

The original design of the Internet was intended for 256 computer networks in the United States. Today, the Internet is a constellation of more than 135,000 networks throughout the world and growing. It is estimated that one-fifth of the American population is already connected to the Internet. The number of worldwide Internet users tripled between 1993 and 1995, to somewhere between 40 and 60 million users. There will be a quarter billion regular users by the year 2000. About 100 countries have Internet access, with 22 joining in 1995. There were fewer than 30,000 Internet-linked computer networks 2 years ago. Today, there are more than 90,000.

In an "Issue Update On Information Security and Privacy in Network Environments" produced by the now disbanded Office of Technology Assessment under the section on safeguarding unclassified information in Federal Agencies it states that, "The need of congressional oversight of federal information security and privacy is even more urgent in time of government reform and streamlining. When the role, size, and structure of the federal agencies are being reexamined, it is important to take into account both the additional information that security and privacy risks incurred in downsizing, and the general lack of commitment on the part of top agency management to safeguarding unclassified information."

The Department of Defense's computer systems are attacked every day according to a GAO Report on Information Security. The Defense Information Systems Agency [DISA] estimates that in 1995 as many as 250,000 attacks may have occurred.

The need to provide guidance to agencies regarding computer security and encryption for Government which is reliable and adequate for the information it is intended to protect, is well established.

I support the need to provide an escrow system for the encryption that is used on Government systems whether they be mainframes or desktop personal computers. These machines are not for private use nor should they be considered personal property. They are purchased and maintained at taxpayer expense and the information they contain is our responsibility to protect.

This legislation would also provide important information on the state of encryption abroad. This will allow us to plan better for a stronger economy and heightened security for information and systems.

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) H7297 2002

Overall, the goals of encryption and its use in the Federal Government may offer the measure of protection needed to secure computers from unwanted intrusions.

I urge my colleagues to vote in favor of H.R. 1903.

Mr. GORDON. Mr. Speaker, I have no additional requests for time, and I yield back the balance of my time.

Mr. SENSENBRENNER. Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore (Mr. LAHOOD). The question is on the motion offered by the gentleman from Wisconsin [Mr. SENSENBRENNER] that the House suspend the rules and pass the bill, H.R. 1903, as amended.

The question was taken.

Mr. CONDIT. Mr. Speaker, I object to the vote on the ground that a quorum is not present and make the point of order that a quorum is not present.

The SPEAKER pro tempore. Pursuant to clause 5, rule I, and the Chair's prior announcement, further proceedings on this motion will be postponed.

The point of no quorum is considered withdrawn.

GENERAL LEAVE

Mr. SENSENBRENNER. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks on H.R. 1903.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Wisconsin?

There was no objection.

EARTHQUAKE HAZARDS REDUCTION ACT OF 1977 AUTHORIZATION

Mr. SENSENBRENNER. Mr. Speaker, I move to suspend the rules and pass the Senate bill (S. 910) to authorize appropriations for carrying out the Earthquake Hazards Reduction Act of 1977 for fiscal years 1998 and 1999, and for other purposes.

The Clerk read as follows:

S. 910

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

SECTION 1. AUTHORIZATION OF APPROPRIATIONS.

Section 12 of the Earthquake Hazards Reduction Act of 1977 (42 U.S.C. 7706) is amended—

(1) in subsection (a)(7)—

(A) by striking "and" after "1995,"; and

(B) by inserting before the period at the end the following: ", $20,900,000 for the fiscal year ending September 30, 1998, and $21,500,000 for the fiscal year ending September 30, 1999";

(2) in subsection (b)—

(A) by striking "and" after "September 30, 1995;";

(B) by inserting before the period at the end the following: "; $52,565,000 for the fiscal year ending September 30, 1998, of which $3,800,000 shall be used for the Global Seismic Network operated by the Agency; and $54,052,000 for the fiscal year ending September 30, 1999, of which $3,800,000 shall be used for the Global Seismic Network operated by the Agency"; and

(C) by adding at the end the following: "Of the amounts authorized to be appropriated under this subsection, at least—

"(1) $8,000,000 of the amount authorized to be appropriated for the fiscal year ending September 30, 1998; and

"(2) $8,250,000 of the amount authorized for the fiscal year ending September 30, 1999,

shall be used for carrying out a competitive, peer-reviewed program under which the Director, in close coordination with and as a complement to related activities of the United States Geological Survey, awards grants to, or enters into cooperative agreements with, State and local governments and persons or entities from the academic community and the private sector.";

(3) in subsection (c)—

(A) by striking "and" after "September 30, 1995,"; and

(B) by inserting before the period at the end the following: ", (3) $18,450,000 for engineering research and $11,920,000 for geosciences research for the fiscal year ending September 30, 1998, and (4) $19,000,000 for engineering research and $12,280,000 for geosciences research for the fiscal year ending September 30, 1999"; and

(4) in the last sentence of subsection (d)—

(A) by striking "and" after "September 30, 1995,"; and

(B) by inserting before the period at the end the following: ", $2,000,000 for the fiscal year ending September 30, 1998, and $2,060,000 for the fiscal year ending September 30, 1999".

SEC. 2. AUTHORIZATION OF REAL-TIME SEISMIC HAZARD WARNING SYSTEM DEVELOPMENT, AND OTHER ACTIVITIES.

(a) AUTOMATIC SEISMIC WARNING SYSTEM DEVELOPMENT.—

(1) DEFINITIONS.—In this section:

(A) DIRECTOR.—The term "Director" means the Director of the United States Geological Survey.

(B) HIGH-RISK ACTIVITY.—The term "high-risk activity" means an activity that may be adversely affected by a moderate to severe seismic event (as determined by the Director). The term includes high-speed rail transportation.

(C) REAL-TIME SEISMIC WARNING SYSTEM.—The term "real-time seismic warning system" means a system that issues warnings in real-time from a network of seismic sensors to a set of analysis processors, directly to receivers related to high-risk activities.

(2) IN GENERAL.—The Director shall conduct a program to develop a prototype real-time seismic warning system. The Director may enter into such agreements or contracts as may be necessary to carry out the program.

(3) UPGRADE OF SEISMIC SENSORS.—In carrying out a program under paragraph (2), in order to increase the accuracy and speed of seismic event analysis to provide for timely warning signals, the Director shall provide for the upgrading of the network of seismic sensors participating in the prototype to increase the capability of the sensors—

(A) to measure accurately large magnitude seismic events (as determined by the Director); and

(B) to acquire additional parametric data.

(4) DEVELOPMENT OF COMMUNICATIONS AND COMPUTATION INFRASTRUCTURE.—In carrying out a program under paragraph (2), the Director shall develop a communications and computation infrastructure that is necessary—

(A) to process the data obtained from the upgraded seismic sensor network referred to in paragraph (3); and

(B) to provide for, and carry out, such communications engineering and development as is necessary to facilitate—

(i) the timely flow of data within a real-time seismic hazard warning system; and

(ii) the issuance of warnings to receivers related to high-risk activities.

(5) PROCUREMENT OF COMPUTER HARDWARE AND COMPUTER SOFTWARE.—In carrying out a program under paragraph (2), the Director shall procure such computer hardware and computer software as may be necessary to carry out the program.

(6) REPORTS ON PROGRESS.—

(A) IN GENERAL.—Not later than 120 days after the date of enactment of this Act, the Director shall prepare and submit to Congress a report that contains a plan for implementing a real-time seismic hazard warning system.

(B) ADDITIONAL REPORTS.—Not later than 1 year after the date on which the Director submits the report under subparagraph (A), and annually thereafter, the Director shall prepare and submit to Congress a report that summarizes the progress of the Director in implementing the plan referred to in subparagraph (A).

(7) AUTHORIZATION OF APPROPRIATIONS.—In addition to the amounts made available to the Director under section 12(b) of the Earthquake Hazards Reduction Act of 1977 (42 U.S.C. 7706(b)), there are authorized to be appropriated to the Department of the Interior, to be used by the Director to carry out paragraph (2), $3,000,000 for each of fiscal years 1998 and 1999.

(b) SEISMIC MONITORING NETWORKS ASSESSMENT.—

(1) IN GENERAL.—The Director shall provide for an assessment of regional seismic monitoring networks in the United States. The assessment shall address—

(A) the need to update the infrastructure used for collecting seismological data for research and monitoring of seismic events in the United States;

(B) the need for expanding the capability to record strong ground motions, especially for urban area engineering purposes;

(C) the need to measure accurately large magnitude seismic events (as determined by the Director);

(D) the need to acquire additional parametric data; and

(E) projected costs for meeting the needs described in subparagraphs (A) through (D).

(2) RESULTS.—The Director shall transmit the results of the assessment conducted under this subsection to Congress not later than 1 year after the date of enactment of this Act.

(c) EARTH SCIENCE TEACHING MATERIALS.—

(1) DEFINITIONS.—In this subsection:

(A) LOCAL EDUCATIONAL AGENCY.—The term "local educational agency" has the meaning given that term in section 14101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 8801).

(B) SCHOOL.—The term "school" means a nonprofit institutional day or residential school that provides education for any of the grades kindergarten through grade 12.

(2) TEACHING MATERIALS.—In a manner consistent with the requirement under section 5(b)(4) of the Earthquake Hazards Reduction Act of 1977 (42 U.S.C. 7704(b)(4)) and subject to a merit based competitive process, the Director of the National Science Foundation may use funds made available to him or her under section 12(c) of such Act (42 U.S.C. 7706(c)) to develop, and make available to schools and local educational agencies for use by schools, at a minimal cost, earth science teaching materials that are designed to meet the needs of elementary and secondary school teachers and students.

(d) IMPROVED SEISMIC HAZARD ASSESSMENT.—

(1) IN GENERAL.—As soon as practicable after the date of enactment of this Act, the

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) H7298 2002

Document No. 58

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [i] 2002

HeinOnline -- 4 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [ii] 2002