In addition, there are estimated to be between 10 and 15 million land mines scattered in the landscape, exploding and injuring at a rate of 20 to 25 per day. They kill or injure predominantly children who are sometimes victims of mines disguised as toys. One out of four Afghan children dies before the age of five. Over one million Afghan children are orphans. Over 500,000 are disabled. Over 400,000 children are amputees, because of land mines. Over one million Afghan children are suffering from post-traumatic stress syndrome.

History has demonstrated that supremacist and totalitarian regimes such as the Taliban militias maintained themselves in power only if the rest of the world remains silent. Human rights are founded on principles that all members of the human family are equal in dignity and rights. However, where discrimination against women and children exists, they are often excluded from effective participation in identifying and securing their rights. In recent years, some have argued that health, defined as ''a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity,'' requires the protection and promotion of human rights. In Afghanistan, Taliban restrictions on Afghan women and children's freedom of expression, association, and movement deny women full participation in society and, consequently, from effectively securing equal opportunities for work, education, and access to health care.

I rise today to reiterate my support for the women and children of Afghanistan. Exclusion of women from employment, and women and children from education, jeopardizes their capacity to survive and participate in society. In my opinion, the health and human rights concerns of Afghan women and children are identified and the promotion of Afghan women and children's health is inseparable from the protection and promotion of human rights.

Ms. JACKSON-LEE of Texas. Madam Speaker, I rise today in strong support of S. 1573, the Afghan Women and Children Relief Act of 2001. This measure would authorize the President to provide educational and health care assistance to the women and children of Afghanistan from funds made available under the 2001 Emergency Supplemental Appropriations Act for Recovery from and Response to Terrorist Attacks on the United States.

The oppression of Afghan women began when the regressive and repressive Taliban took control of Afghanistan. Under the regime of these Islamic fundamentalists, women became subject to a horrific system of gender apartheid whereby the rights enjoyed by women in so many other areas of the world, the rights they are entitled to, were virtually eliminated.

In Afghanistan, women are totally deprived of the right to an education, of the right to work, to travel, to health care, legal recourse, recreation, and of the right to being human. Islamic fundamentalism, instead, looks upon women as subhuman, fit only for household slavery and as a means of procreation. Women who violate the rules of conduct are beaten or brutalized, often in a public arena for the sake of entertainment.

This type of inhumane treatment will have a profound effect on the future of Afghanistan. As Chair of the Congressional Children's Caucus, I am always concerned about the welfare of children here at home and abroad. Young Afghan girls are also subject to the extreme restrictions imposed by the Taliban—restrictions to education, health care, and a normal way of life. Afghan children are some of the poorest and least healthy in the world. They have the highest mortality rates for children under five. These children have known only war, so they are suffering enormous trauma as well.

As the Taliban regime retreats from the major Afghanistan cities, the masses are rejoicing at the hope of renewed opportunities for the country. The talents and contributions of Afghan women will once again permeate the country. Prior to the Taliban regime, seventy percent of teachers were women, fifty percent of civil servants were women, and university students, and forty percent of doctors were women. This bill will assure that women and children are able to exercise their right to education and healthcare.

Madam Speaker, we, as Members of Congress, now have a tool to help restore the rights and human dignity of Afghan women and children. I urge my colleagues to support S. 1573.

Ms. SOLIS. Madam Speaker, I rise today in support of S. 1573.

I am an educated woman. Not only do I hold an undergraduate degree, I also have earned a master's degree.

I am a healthy woman. Not only do I receive regular medical care from my physician, I also have access to superb emergency care if needed.

I am an independent woman. Not only do I have a challenging career, I also feel secure strolling the streets of this city alone.

Such is not the case, however, for the women and girls of Afghanistan.

During the days of Taliban rule, these women were denied education. They were denied health care. They were denied basic human freedoms.

In these emerging days of post-Taliban rule, it is our duty to ensure that these basic civil liberties are restored.

I commend the authors of S. 1573—and its companion legislation H.R. 3330—for their aim of providing education and health care opportunities to the women and children of Afghanistan. I especially applaud the desire to utilize women-led non-governmental organizations to achieve their goals.

I urge all of my colleagues on both sides of the aisle to support this important piece of legislation.

Ms. HARMAN. Madam Speaker, I rise in strong support of H.R. 3330, the Afghan Women And Children Relief Act. This legislation will ensure that educational and health care assistance reaches the women and children of Afghanistan.

The Taliban's crimes against women have by now become well-known. Against the teaching of Islam and against the will of women across Afghanistan, the Taliban:

Ended education for girls over eight;

Shut down the women's university;

Forbade women doctors from practicing medicine; and

Then forbade women from receiving care from male doctors.

This deliberate, cruel treatment compounded the suffering of more than 20 years of war, extreme poverty, and drought in Afghanistan to create a dire health situation for women and children. Afghanistan has the world's second worst maternal death rate during childbirth. One hundred sixty five out of every thousand babies die before their first birthday. The Taliban has done untold harm to its own people with these actions, and we must now help repair the damage done.

Rebuilding Afghanistan is part of the promise we have made to provide a comprehensive solution to the root causes of terrorism. We must offer hope to the people of Afghanistan, and we must work toward creating a stable Afghan government.

Aid to the women and children of Afghanistan will accomplish both of these goals. It will improve the lives of millions and increase opportunities for all members of Afghan society—including women—to have their voices heard.

The overwhelming bipartisan support by Congress today demonstrates that our support is no short-term political ploy. We are here for the long haul, and we expect to see results.

Ms. BERKLEY. Madam Speaker, I have no further requests for time, and I yield back the balance of my time.

The SPEAKER pro tempore (Mrs. BIGGERT). The question is on the motion offered by the gentlewoman from Florida (Ms. ROS-LEHTINEN) that the House suspend the rules and pass the Senate bill, S. 1573.

The question was taken; and (two-thirds having voted in favor thereof) the rules were suspended and the Senate bill was passed.

A motion to reconsider was laid on the table.

COMPUTER SECURITY ENHANCEMENT ACT OF 2001

Mrs. MORELLA. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 1259) to amend the National Institute of Standards and Technology Act to enhance the ability of the National Institute of Standards and Technology to improve computer security, and for other purposes, as amended.

The Clerk read as follows:

H.R. 1259

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

SECTION 1. SHORT TITLE.

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

SEC. 2. FINDINGS AND PURPOSES.

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

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

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

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

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

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

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

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

SEC. 3. SECURITY OF FEDERAL COMPUTERS AND NETWORKS.

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

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

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

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

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

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

SEC. 4. COMPUTER SECURITY IMPLEMENTATION.

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

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

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

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

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

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

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

''(D) upon the request of a Federal agency, perform evaluations to assess its existing information security and privacy programs;

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

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

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

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

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

''(2) The Institute shall maintain and make available to Federal agencies and to the public a list of commercially available security products that have been tested by private sector laboratories certified in accordance with procedures established under paragraph (1)(G)(ii), and that have been found to be in conformance with the guidelines and standards developed under subsection (a)(2) and (3).

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

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

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

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

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

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

''(d)(1) The Institute shall solicit the recommendations of the Computer System Security and Privacy Advisory Board, established by section 21, regarding standards and guidelines that are being considered for submittal to the Secretary in accordance with subsection (a)(4). The recommendations of the Board shall accompany standards and guidelines submitted to the Secretary.

''(2) There are authorized to be appropriated to the Secretary $1,030,000 for fiscal year 2002 and $1,060,000 for fiscal year 2003 to enable the Computer System Security and Privacy Advisory Board, established by section 21, to identify emerging issues related to computer security, privacy, and cryptography and to convene public meetings on those subjects, receive presentations, and publish reports, digests, and summaries for public distribution on those subjects.''.

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

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

''(g) The Institute shall not promulgate, enforce, or otherwise adopt standards or policies for the Federal establishment of encryption and electronic authentication standards required for use in computer systems other than Federal Government computer systems.''.

SEC. 7. MISCELLANEOUS AMENDMENTS.

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

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

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

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

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

SEC. 8. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.

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

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

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

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

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

SEC. 9. COMPUTER SECURITY FELLOWSHIP PROGRAM.

There are authorized to be appropriated to the Secretary of Commerce $5,000,000 for fiscal year 2002 and $5,000,000 for fiscal year 2003 for the Director of the National Institute of Standards and Technology for fellowships, subject to the provisions of section 18 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–1), to support students at institutions of higher learning in computer security. Amounts authorized by this section shall not be subject to the percentage limitation stated in such section 18.

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

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

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

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

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

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

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

(c) INTERAGENCY COOPERATION WITH STUDY.—All agencies of the Federal Government shall cooperate fully with the National Research Council in its activities in 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 electronic authentication technologies for use by individuals, businesses, and government. The National Research Council shall not recommend the implementation or application of a specific electronic authentication technology or electronic authentication technical specification for use by the Federal Government. Such report shall be submitted in unclassified form.

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

SEC. 11. PROMOTION OF NATIONAL INFORMATION SECURITY.

The Under Secretary of Commerce for Technology shall—

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

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

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

SEC. 12. ELECTRONIC AUTHENTICATION INFRASTRUCTURES.

(a) ELECTRONIC AUTHENTICATION INFRASTRUCTURES.—

(1) TECHNOLOGY-NEUTRAL GUIDELINES AND STANDARDS.—Not later than 18 months after the date of the enactment of this Act, the Director, in consultation with industry and appropriate Federal agencies, shall develop technology-neutral guidelines and standards, or adopt existing technology-neutral industry guidelines and standards, for electronic authentication infrastructures to be made available to Federal agencies so that such agencies may effectively select and utilize electronic authentication technologies in a manner that is—

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

(B) interoperable, to the maximum extent possible.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SEC. 13. SOURCE OF AUTHORIZATIONS.

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

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from Maryland (Mrs. MORELLA) and the gentleman from Texas (Mr. HALL) each will control 20 minutes.

The Chair recognizes the gentlewoman from Maryland (Mrs. MORELLA).

GENERAL LEAVE

Mrs. MORELLA. Madam Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks on H.R. 1259.

The SPEAKER pro tempore. Is there objection to the request of the gentlewoman from Maryland?

There was no objection.

Mrs. MORELLA. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, it is with great pleasure that I rise to offer H.R. 1259, the Computer Security Enhancement Act of 2001. This legislation represents many years of bipartisan work of the Committee on Science. Over the years, the committee has held numerous hearings on various aspects of the bill's provisions and has incorporated many constructive suggestions made by both industry and governmental agencies. This bill provides important updates to current law to ensure the Federal Government's virtual security.

Fourteen years ago, this body passed the Computer Security Act of 1987, which gave authority over computer and communication security standards for Federal civilian agencies to the National Institute for Standards and Technology. Much has changed since then. In the mid-eighties, we were dealing with issues surrounding the migration from mainframes to personal computers and how to provide secure access to extremely limited, site-specific internal networks. Today, with the worldwide web, every PC on the planet represents a potential source of attack, and we need to develop new tools to protect the integrity of our Nation's computers.

While no single piece of legislation can fully protect our Federal computer systems, this act is a vital step to strengthen and update the authority given the National Institute of Standards and Technology to provide guidance to our security efforts.

This bill is an important first step in the right direction. The legislation would allow NIST to: promote the use of commercially available, off-the-shelf security products by Federal agencies; increase privacy protection by giving an independent advisory board more responsibility and resources to review NIST's computer security efforts and make recommendations; support the development of a well-trained workforce by creating a fellowship program in the field of computer security; study the efforts of the Federal Government to develop a secure, interoperable electronic infrastructure; to advise agencies on the deployment of electronic authentication technologies; and, finally, establish an expert review team to assist agencies in identifying and fixing existing information security vulnerabilities.

In today's environment, the intense need for this legislation is obvious. For the last few months, we have been frantically trying to recover from the awful attacks of September 11 and plug the many holes in our society's lax security practices. We have gone to great effort to quickly react to vulnerabilities on many fronts. We passed legislation to secure much of our important infrastructure, and the administration has moved forward with many counterterrorism proposals. But, along with the real world, we need to protect ourselves in cyberspace.

Fortunately, we have not suffered a major cyberattack, but that is hardly a reason not to act. A major cyberoffensive could be every bit as devastating as an actual physical assault. A full third of our recent economic development has been credited to e-commerce and needs to be secure. Never before has so much of our daily lives been documented and placed on Federal computers. Americans have the right to expect that this information does not fall into the wrong hands.

Unfortunately, the government is not very adept at protecting this information. Over the last decade, the General Accounting Office has issued nearly 40 reports describing serious information

security weaknesses at major Federal agencies. Our own House Committee on Government Reform has recently issued its computer security report card and given the government an ''F.''

Quite frankly, this is unacceptable. Now is the time to expand NIST's authority so we can begin to address these issues.

Located in my home district of Montgomery County, NIST already plays a critical control role in our Nation's computer security. They are our Nation's premier developer of standards and guidelines and have worked tirelessly in the information technology area. They work closely with industry, Federal agencies, testing organizations, academicians and other private sector users with the broad mission of improving our competitiveness in IT and computer-related industries.

Specifically, they work to improve awareness of computer security issues, conduct research on new cutting-edge technologies, develop and manage security testing programs, and produce security guidance and planning.

Madam Speaker, I am very proud of their work in this area. They have a well-deserved reputation for excellence and deserve the additional resources to expand their efforts in computer security. They are the recognized leader in this field and the logical choice to coordinate and critique the government's efforts.

Madam Speaker, a wide array of technology organizations have recognized the need for H.R. 1259 to protect our Nation's computer systems and secure our virtual presence. I thank them for their support. I urge my colleagues to stand with these organizations and take the important step towards securing our computer data and resources by passing H.R. 1259.

Madam Speaker, I reserve the balance of my time.

Mr. HALL of Texas. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise today in support of H.R. 1259; and, in her usual good practice, the gentlewoman from Maryland (Mrs. MORELLA) has very well outlined the provisions of the legislation. I would just like to make a few observations concerning the need for the legislation before us today.

The Committee on Science developed the Computer Security Act 13 years ago with the goal in mind of improving the security of nonclassified information in the Federal agencies' computer systems. When Congress passed the Computer Security Act back in 1987, most of us realized that this new method of communication needed to be secure in order to realize the full potential that those that brought it forth had hoped for. At that time we had no idea of the growth of the Internet, electronic commerce, or even the growth of e-mail communication from our constituents. In the past few years, the spread of computer viruses, attacks by computer hijackers and electronic identification theft have all been on the rise. Regardless of our reliance on the Internet and computer networks, computer security is still generally regarded as an afterthought.

On September 11, we realized how very vulnerable our Nation could be. We no longer can afford to be complacent about our physical and electronic security. Hearings by the Committee on Science and assessments by the General Accounting Office have revealed that computer security at Federal levels is still, in many people's opinion, sub par.

The National Institute of Standards and Technology has an important role to play here. It is responsible for developing security standards and developing the very best security practices. It should assist agencies in training their computer security personnel and help assess their security weaknesses.

Unfortunately, NIST has never really requested nor received the resources it needs to effectively carry out their statutory role in these areas. The Committee on Science has developed this bipartisan legislation to correct this problem. The goal of this legislation is to strengthen the computer security of Federal agencies, including, of course, the use of electronic authentication technologies.

H.R. 1259 is not merely in response to the events of September 11. Actually, H.R. 1259 is and has been a result of continued and careful study and deliberation by the Committee on Science. We began work on this legislation at the beginning of the last Congress, and it has been the subject of hearings, and we have asked for comments by industry and Federal agencies. It is a thoughtful and straightforward approach for making Federal agencies a model of good security practices.

I congratulate the gentlewoman from Maryland (Mrs. MORELLA), the gentleman from Tennessee (Mr. GORDON), and the gentleman from Michigan (Mr. BARCIA) for their hard work on this legislation. Also, we would not be here without the assistance and support of the gentleman from New York (Chairman BOEHLERT) and his efforts to bring this bill to the floor. This a timely piece of legislation, Madam Speaker, and I would urge my colleagues to support the bill.

Madam Speaker, I reserve the balance of my time.

Mrs. MORELLA. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I commend the ranking member, the gentleman from Texas (Mr. HALL), for his leadership. Together we are a team. The Committee on Science is a very bipartisan, almost nonpartisan committee, and it is my pleasure to thank the gentleman from Texas and the gentleman from New York (Chairman BOEHLERT).

Madam Speaker, I yield such time as he may consume to the gentleman from New York (Mr. BOEHLERT), the chairman of the Committee on Science, and commend him for his leadership.

Mr. BOEHLERT. Madam Speaker, I thank the gentlewoman for yielding me this time.

Madam Speaker, I rise to support H.R. 1259, the Computer Security Enhancement Act of 2001, and to congratulate the gentlewoman from Maryland (Mrs. MORELLA) and the gentleman from Texas (Mr. HALL) and the gentleman from Tennessee (Mr. GORDON) for their bipartisan work on this legislation and for the leadership of the past chairman, the gentleman from Wisconsin (Mr. SENSENBRENNER), who shepherded this bill through the House in the last Congress.

Since the tragedy of September 11, our Nation has awakened to a new world of potential threats. Some of them before now were thought not possible. Some were thought not likely. And, unfortunately, some were simply ignored. But in the last 2 months, the world has changed and we have resolved to fortify our Nation's critical assets, to protect our airports and strengthen our infrastructure.

One compelling need is to improve the security of our Nation's computer systems and the uncountable government services on which they depend. In the last 9 years, the General Accounting Office has issued some three dozen reports detailing the serious information security weaknesses at major Federal agencies. We in the House, and particularly on the Committee on Science, have heeded these warnings. Others must, also.

□ 1500

Federal systems are not the only ones central to our Nation's smooth functioning. Earlier this year, the Committee on Science held several hearings on cybersecurity. In one of those, Governor Gilmore testified that his commission, which was charged with evaluating our Nation's vulnerabilities to weapons of mass destruction, could not ignore the potential additional havoc that computer attacks could wreak on our country, especially if computer attacks were launched at the same time as some other attack. Computer breaches must not be allowed to hamstring State and local governments as they attempt to respond to other kinds of threats.

This bill, the first of several dealing with cybersecurity that the Committee on Science plans to bring to the floor, begins to make the kinds of improvements necessary to address the concerns these reports have raised. H.R. 1259 will encourage the computer security teams at the National Institute of Standards and Technology to assist other government agencies to improve the security of their computer networks. It will spur the private sector to develop improved computer security products to benefit the public and private sectors alike. And it will help recruit and train future experts in the profession of computer security.

I would also like to point out that this very same bill passed this body a

little over a year ago. Unfortunately, the other body did not have time to pass it and send it on to the President. This time, however, I hope we can work with our colleagues in the Senate to pass this bill to strengthen our Nation's computer security and to help protect the American people.

This bill is a good bill that will help our Nation deal with a serious threat that for too long has been inadequately addressed. I urge my colleagues to support this bill and help put our Nation on the road to better computer security.

In closing, let me once again commend the leadership of the gentlewoman from Maryland and the bipartisan team that she has assembled and led as we have moved this through the committee and now to the House floor. I hope others are paying attention, because they need to follow through.

Mr. HALL of Texas. Madam Speaker, I yield such time as he may consume to the gentleman from Tennessee (Mr. GORDON), who was ranking member on the Subcommittee on Environment, Technology, and Standards back when this legislation first began and wrote the electronic authentication provisions in it. He is now ranking member on the Subcommittee on Space and Aeronautics.

Mr. GORDON. Madam Speaker, I thank the gentleman from Texas (Mr. HALL) for yielding time, and more importantly I thank him for the leadership he brings to the Committee on Science.

Madam Speaker, I want to thank the gentlewoman from Maryland (Mrs. MORELLA) and the gentleman from New York (Mr. BOEHLERT) for their diligent work to bring this bill to the floor today. When the gentlewoman from Maryland and I began to work to improve Federal agencies' nonclassified computer security more than 4 years ago, I became aware that an important element of any computer security regime is electronic authentication.

Consistent with the goals of the Government Paperwork Elimination Act, I wanted to ensure that Federal agencies deployed electronic authentication technologies in a consistent and uniform manner and that there was a reasonable level of interoperability between electronic authentication systems deployed by Federal agencies.

Federal agencies have made some progress on improved computer security since the Committee on Science began working on this issue. However, significant vulnerabilities remain and much work needs to be done. Earlier this year, the GAO documented continued computer security failings of Federal agencies. And just a few weeks ago, a Committee on Government Reform assessment of Federal agencies' computer security was uniformly dismal.

The events of September 11 made it evident that we cannot remain so complacent and lax about the security of electronic documents and transactions. The disruption of traditional document carriers like our mail and airline systems highlighted that we need to be able to transfer documents over an open and secure electronic communications system. Such a system must include robust and widely deployed electronic authentication technologies. Unfortunately, electronic authentication technologies have yet to be widely used. One of the goals of this bill is to ensure the effective deployment of electronic authentication technologies by Federal agencies.

The Computer Security Enhancement Act is the result of discussions with industry, the National Institute of Standards and Technology, and the Department of Commerce. Under the bill, NIST, working with industry, is to develop minimum technical standards and guidelines to assist Federal agencies in deploying electronic authentication technologies. It is my intent that Federal agencies serve as models of how such technologies could be effectively implemented.

I want to clarify that NIST is not developing standards but only guidelines and best practices. When I drafted these provisions relating to electronic authentication, I tried to ensure that the private sector would have a strong voice in the development of any guidelines. NIST has a strong record of working cooperatively with industry. I believe the result will be greater security and lower cost for everyone as we move toward an electronic transaction-based economy.

Finally, Madam Speaker, I want to thank all the staff that have spent so many hours on this bill, particularly Mike Quear that assisted me on the bill. As they did in the 106th Congress, I would urge my colleagues to again support this legislation.

Mr. HALL of Texas. Madam Speaker, I have no further requests for time, and I yield back the balance of my time.

Mrs. MORELLA. Madam Speaker, I yield myself such time as I may consume.

It appears as though everyone recognizes the need for this bill and is in support of it. In addition to the numerous technology organizations that have indicated their strong support and have worked on the bill through the years, the President's Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction chaired by Governor Gilmore has called for an expanded role for NIST. That is what this bill does.

I urge my colleagues to stand with these organizations and take an important step toward securing our computer data and resources by passing H.R. 1259. I also want to add my thanks to the gentleman from Tennessee (Mr. GORDON). He was my ranking member on the Subcommittee on Environment, Technology, and Standards when this bill was crafted. I thank him for his important contributions. Again I reiterate my thanks to ranking member HALL, to Chairman BOEHLERT, to the gentleman from Michigan (Mr. BARCIA), who also served on that subcommittee, and certainly the staff on both sides of the aisle. I want to commend Barry Beringer and certainly thank Ben Wu, who was my staffer who is no longer with us but is now the Deputy Under Secretary of Science and Technology at the Department of Commerce, Carl Piccanatto from the National Academy of Science, Jason Cervenak and the various staff that we have again on both sides of the aisle. I urge everyone to support H.R. 1259.

Ms. JACKSON-LEE of Texas. Madam Speaker, I rise in support of this legislation H.R. 1259, the Computer Security Enhancement Act of 2001.

In the world of technology today, interactive computer applications are a standard worldwide and virtually anyone in the world can gain access to government information. A lack of security in the computer systems of key government agencies is a vulnerability that has persisted for too long and will still be around if it is not dealt with at once. The number of attacks have soared in recent years and it is not just hackers and terrorists that we have to be worried about, but foreign governments and other nation states as well. Less than 3 years ago, the Federal Computer Incident Response Center calculated 376 occurrences upsetting 2,732 Federal systems and 86 military systems. Last year, the number of incidents reported was 586, which involved 575,568 Federal systems and 148 military systems.

A few months ago, Chinese hackers invaded government and business Web sites, including those run by the Navy and the Departments of Labor and Health and Human Services. Last year, a program called, ''ILOVEYOU'' penetrated systems at the Defense Department, the CIA and at least a dozen other agencies, attacking their infrastructure and networks.

There is a clear risk that exists, as computer strikes become more sophisticated. Terrorists or hostile foreign states could unleash attacks through computers, severely damaging or disrupting systems that support critical infrastructure. This can lead to disorder in our Nation's defense and public operations or stolen data of sensitive material. The disturbing element is that the vast majority of these kinds of incidents are never reported, in part, because some agencies cannot detect when a hacker has even gained access to their files.

H.R. 1259, Computer Security Enhancement Act of 2001 will amend the National Institute of Standards and Technology Act by requiring the Institute to provide assistance to Federal agencies. The assistance will include developing cost-effective and uniform standards for the security and privacy of sensitive information in certain Federal systems, providing a list of certified commercial Federal computer system security products, and reporting annually on Federal computer system evaluations. Their aid will be used to protect computer networks, promote Federal compliance with computer information security and privacy guidelines, as well as assist Federal response efforts when there is unauthorized access to Federal systems.

H.R. 1259 will focus the energy of the Institute as well as agencies' such as the National Research Council of he National Academy of

Sciences and the Undersecretary of Commerce for Technology on security and encryption issues. Studies, training, and adoption of standards and products will be developed.

This bill will also authorize appropriations for fellowships to students in computer security. There is a need for specialists in the United States and this bill will hopefully be part of a solution to the growing shortage of security professionals within government and this industry.

According to government reports, 24 Federal agencies, have not adopted effective security to protect their computers and networks from attacks. Many agencies still do not use passwords properly and cannot detect intruders. Federal agencies who support this bill: the Defense Department, the Departments of Labor and Health and Human Services, the CIA, the Department of Transportation, Departments of Justice, State and the Treasury, Nuclear Regulatory Commission, U.S. Army Corps of Engineers, the Environmental Protection Agency, the Commerce Department as well as the Federal Aviation Administration.

On a particular occasion last year, a computer virus breached the Defense Department's security system, damaging some computers and infecting several classified systems. Computer attacks could disable sensitive operations such as the FAA flight control system or Pentagon war efforts. This disruption could have chaotic consequences.

This bill is a step forward in combating our current vulnerability of a lack of proper protection on Federal computer systems. With the passing of this bill will come Federal standards that will implement much needed assistance and programs. It is an imperative part of a solution to better respond to current attacks as well as potential ones.

Mr. SMITH of Michigan. Madam Speaker, I rise in strong support of this legislation, offered by the gentlewoman from Maryland, to strengthen the security of sensitive Federal computer systems.

Information security has taken on new significance. Today, the economy and our national security rely on computers as never before. Protecting these systems by reducing their vulnerability to cyber-attack must therefore be a high priority. The same techniques that agencies are employing to cut costs and improve public services—interconnected systems, readily accessible information, and paperless processing—are also factors that increase the vulnerability of these systems to hackers.

Key strengths of this bill are its emphasis on cost-effective solutions and government adoption of commercially available products. Equally important are provisions to address privacy issues and ensure public participation in the development of guidelines. I would emphasize the bill does not mandate Federal guidelines or standards for the private sector.

In a series of hearings held by the Science Committee, we learned a great deal about the existing and emerging threats to computer systems. Despite these threats, there is relatively little university-based research.

The computer security fellowship program in this bill is a start. I plan to move an information technology research bill that will increase cyber-security research even further.

As a senior member of the Science Committee, the gentlewoman from Maryland has produced an important piece of legislation that is very much needed. I urge my colleagues to support it.

Mrs. MORELLA. Madam Speaker, I yield back the balance of my time.

The SPEAKER pro tempore (Mrs. BIGGERT). The question is on the motion offered by the gentlewoman from Maryland (Mrs. MORELLA) that the House suspend the rules and pass the bill, H.R. 1259, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds of those present have voted in the affirmative.

Mrs. MORELLA. Madam Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX and the Chair's prior announcement, further proceedings on this motion will be postponed.

RECOGNIZING JOSEPH HENRY FOR HIS ROLE IN DEVELOPMENT OF SCIENCE AND ELECTRICITY

Mrs. MORELLA. Madam Speaker, I move to suspend the rules and agree to the concurrent resolution (H. Con. Res. 157) recognizing and honoring Joseph Henry for his significant and distinguished role in the development and advancement of science and electricity.

The Clerk read as follows:

H. CON. RES. 157

Whereas Joseph Henry was born December 17, 1797, in Albany, New York, the son of William and Ann Henry;

Whereas Joseph Henry served as an apprentice to John Doty, a watchmaker and jeweler, in preparation for attendance at the Albany Academy;

Whereas from 1819 to 1822, Joseph Henry attended advanced classes at the Albany Academy and, in the spring of 1826, was elected to the professorship of Mathematics and Natural Philosophy in the Albany Academy;

Whereas Joseph Henry revolutionized scientific education by using experiment-based teaching methods at the Albany Academy, and in 1829 was awarded an honorary Masters degree by Union College, despite having no formal college education;

Whereas Joseph Henry conducted many experiments with electromagnets, which led to his successful design and construction of an electromagnet capable of lifting 750 pounds;

Whereas Joseph Henry continued to improve upon the development of the electromagnet, building an electromagnet for Yale University in 1831 that was capable of lifting 2,300 pounds, and another electromagnet, known as ''Big Ben'', that was capable of lifting 3,500 pounds, which was, at the time that it was built in 1833, the most powerful electromagnet ever built;

Whereas in January 1831, Joseph Henry helped lay the groundwork for the development of the electromagnetic telegraph by distinguishing between quantity and intensity magnets and by publishing those findings in the American Journal of Science;

Whereas the modern practical unit of induction is commonly referred to as the ''Henry'' in honor of Joseph Henry's research and discoveries regarding self-induction;

Whereas Joseph Henry, while conducting research at the Albany Academy, invented an electromagnetic motor made of a horizontally poised bar electromagnet that would rock back and forth as the current through it was automatically reversed;

Whereas Joseph Henry, while serving as Professor of Natural Philosophy in the College of New Jersey at Princeton (currently known as ''Princeton University''), conducted experiments from 1838 to 1842 which laid the theoretical groundwork for modern step-up and step-down transformers;

Whereas, on December 14, 1846, Joseph Henry was selected as the first Secretary and Director of the Smithsonian Institution;

Whereas, in his first report to the Board of Regents of the Smithsonian Institution, Joseph Henry proclaimed that the purpose of the Smithsonian Institution, the increase and diffusion of knowledge among men, would be best achieved by supporting original research and providing for the wide distribution of the most recent findings in the various fields of natural sciences;

Whereas in 1850 Joseph Henry, as Secretary of the Smithsonian Institution, established the system of receiving weather reports by telegraph and utilizing such reports to predict weather conditions and issue storm warnings;

Whereas in 1869 Congress established a national weather bureau upon the recommendation of Joseph Henry;

Whereas Joseph Henry was appointed as a member of the Light House Board in 1852, and served as its president from 1871 until his death in 1878;

Whereas Joseph Henry was an original member of the National Academy of Sciences, its vice-president in 1866, and its president from 1868 until his death in 1878;

Whereas Joseph Henry died in the District of Columbia on May 13, 1878;

Whereas a memorial service was held in honor of Joseph Henry on January 16, 1879, in the Hall of the House of Representatives, and was attended by the President, Vice President, members of the President's Cabinet, Justices of the Supreme Court, Members of Congress, and members of the Board of Regents of the Smithsonian Institution; and

Whereas the memory of Joseph Henry was honored at the opening of the Library of Congress in 1890 by including a statue of Joseph Henry among the 16 bronze portrait statues on display which represent human development and civilization: Now, therefore, be it

Resolved by the House of Representatives (the Senate concurring), That Congress recognizes and honors Joseph Henry for his significant and distinguished role in the development and advancement of science and electricity.

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from Maryland (Mrs. MORELLA) and the gentleman from Texas (Mr. HALL) each will control 20 minutes.

The Chair recognizes the gentlewoman from Maryland (Mrs. MORELLA).

GENERAL LEAVE

Mrs. MORELLA. Madam Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and include extraneous material on the concurrent resolution now under consideration.

The SPEAKER pro tempore. Is there objection to the request of the gentlewoman from Maryland?

There was no objection.

Mrs. MORELLA. Madam Speaker, I yield myself such time as I may consume. I rise in support of House Concurrent Resolution 157. I commend my