Support Program. I was very pleased the Committee adopted the amendment I offered to boost the authorizing level of this program to $125 million. This funding level is vital. About 4.4 million people in the United States over the age of 65 require long-term care due to a functional disability. All too often the needs of older Americans and the family members that care for them create an undue burden on the quality of life of the entire family. This legislation would authorize $125 million to establish a new program that would provide grants to states for supporting the crucial role of family members in the care of their loved ones, by, for example, providing respite care and adult care to complement the care provided by family.

The National Family Caregiver Support Program is just one of the many initiatives in the Older Americans Act that promises to improve the lives of some of our nation's neediest and most neglected citizens. I urge my colleagues to stand with me in support of this important legislation. We owe it to our nation's seniors.

Mr. KIND. Mr. Speaker, I am pleased to rise in support of the Older Americans Act Amendments of 2000 (H.R. 782). It is impressive that during the waning days of Congress, we could reach a bipartisan, bicameral agreement on this important legislation.

Since its enactment more than thirty years ago, the Older Americans Act has enabled millions of older persons, especially those with disabilities, to remain independent and productive. Many of these individuals would have been institutionalized were it not for the home and community-based services such as meals and transportation provided by the landmark legislation. The nutrition programs, including Meals on Wheels, provided about 240 million congregate and home-delivered meals last year to more than three million of our nation's senior citizens. Older Americans have also benefited from the Senior Community Service Employment program that provides on-the-job-training for those who needs work.

As a member of the Committee on Education and the Workforce, I have worked diligently with my colleagues to reach a consensus on reauthorization, and this legislation before us addresses a number of critical issues. One of the biggest debates during committee consideration was funding for the Senior Community Service Employment program. H.R. 782 ensures that no state will receive less than it received in FY2000 and every state is guaranteed a certain percentage of any new money that is appropriate above the FY2000 level. In addition, no national organization, such as Green Thumb, will receive less than what is needed to match its effort in FY2000. Further, this legislation continues to target resources to the seniors who are most in need and ensures that funds are more equitably distributed between urban and rural areas.

The size of the elderly population will begin to dramatically increase in the next decade, putting greater demands on the time and energy of family caregivers. We need to explore ways to support our families when they are called upon to fill these vital roles. I am pleased that H.R. 782 includes the National Family Caregiver Support Program. Modeled after efforts begun in Wisconsin and elsewhere, it would provide grants to states for the following services: (1) information to caregivers about available services; (2) assistance to caregivers in gaining access to services; and (3) counseling and training to help families make decisions and solve problems related to their caregiving roles.

I know how important the Older Americans Act is to millions of seniors, particularly those in rural regions such as western Wisconsin. That is why I urge my colleagues to support this bipartisan legislation and demonstrate our continued commitment to our nation's seniors.

Mr. BEREUTER. Mr. Speaker, this Member rises today in strong support of H.R. 782, the Older Americans Act Amendments.

The Older Americans Act has provided care and services to our nation's elderly population through many programs, including meals on wheels, congregate meals, home care, adult day care, senior centers, senior transportation, job training programs, a long term care ombudsman, and abuse prevention and elder rights.

In particular, this Member feels the National Family Caregiver Support Program is an important provision which aids families in caring for their elderly relatives, for grandparents caring for grandchildren and other related children. By providing care and extending the ability of an aging family member to stay at home, family caregivers reduce long-term costs to Medicaid. The ability to provide respite for those who care for an ailing family member has proven to reduce stress and burnout of these individuals who provide such an invaluable service to their family. Services provided through respite include information and assistance in gaining access to services, counseling, support and caregiver training, respite care, and additional supplemental services.

Mr. Speaker, this Member would like to thank my colleague from Nebraska, Mr. BARRETT, for introducing this important piece of legislation. It provides important services that many seniors rely on and this Member encourages my colleagues to support it.

Mr. LOBIONDO. Mr. Speaker, I rise today to congratulate all those who have worked so hard to make the reauthorization of the Older Americans Act (OAA) a reality. This authorization means more than just the mechanics of legislation. It is about senior citizens, and how their lives have been changed for the better by the successful federal, state and local partnerships that have prospered under the OAA.

OAA programs are critical to the long-term benefit of seniors. With the population of senior citizens about to skyrocket with the addition of the ''baby boom'' generation, OAA programs represent a cost-efficient and effective means to provide a community safety net for the elderly. The continuing popularity of Meals-on-Wheels and Green Thumb programs in states—which have been very successful in bringing isolated and idle elderly back into the community fold—are testimony to the continued need for a federal, state, and local partnership oriented to the care of senior citizens.

These are programs I have seen working at home in my Congressional district, located in Southern New Jersey. I have delivered meals to seniors and can tell you from personal experience that the looks on their faces, when we come to their door with a hot meal, is by itself reason enough to reauthorize the OAA. I have seen countless numbers of senior citizens in my district whose lives have been enriched by Green Thumb. In utilizing their ample skills and experience, we are giving seniors a renewed purpose in their lives by offering them a chance to re-join the workforce.

Mr. Speaker, the OAA is a federal program with two essential ingredients: cost-efficiency and a record of success. In short, OAA programs represent a safety net, and have kept seniors from sitting idle and becoming isolated from their community.

By reauthorizing the OAA, Congress will reaffirm its commitment to caring for our seniors and retirees. I am very pleased that this important program will continue to enrich and improve the quality of life of America's seniors.

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

The SPEAKER pro tempore (Mr. HANSEN). The question is on the motion offered by the gentleman from California (Mr. MCKEON) that the House suspend the rules and pass the bill, H.R. 782, as amended.

The question was taken; and the Speaker pro tempore announced that the ayes appeared to have it.

Mr. GOODLING. Mr. 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.

COMPUTER SECURITY ENHANCEMENT ACT OF 2000

Mr. SENSENBRENNER. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 2413) to amend the National Institute of Standards and Technology Act to enhance the ability of the National Institute of Standards and Technology to improve computer security, and for other purposes, as amended.

The Clerk read as follows:

H.R. 2413

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 2000''.

SEC. 2. FINDINGS AND PURPOSES.

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

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

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

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

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

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

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

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

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

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

(1) by redesignating paragraphs (2), (3), (4), and (5) as paragraphs (3), (4), (8), and (9), respectively; and

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

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

SEC. 4. SECURITY OF FEDERAL COMPUTERS AND NETWORKS.

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

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

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

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

SEC. 5. COMPUTER SECURITY IMPLEMENTATION.

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

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

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

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

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

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

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

''(D) perform evaluations and tests at Federal agencies to assess existing information security and privacy programs;

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

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

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

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

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

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

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

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

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

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

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

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

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

''(2) There are authorized to be appropriated to the Secretary $1,030,000 for fiscal year 2001 and $1,060,000 for fiscal year 2002 to enable the Computer System Security and Privacy Advisory Board, established by section 21, to identify emerging issues related to computer security, privacy, and cryptography and to convene public meetings on those subjects, receive presentations, and publish reports, digests, and summaries for public distribution on those subjects.''.

SEC. 7. LIMITATION ON PARTICIPATION IN REQUIRING ENCRYPTION STANDARDS.

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

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

SEC. 8. MISCELLANEOUS AMENDMENTS.

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

(1) in subsection (b)(9), as so redesignated by section 3(1) of this Act, by inserting ''to the extent that such coordination will improve computer security and to the extent necessary for improving such security for Federal computer systems'' after ''Management and Budget)'';

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

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

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

SEC. 9. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.

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

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

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

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

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

SEC. 10. COMPUTER SECURITY FELLOWSHIP PROGRAM.

There are authorized to be appropriated to the Secretary of Commerce $500,000 for fiscal year 2001 and $500,000 for fiscal year 2002 for the Director of the National Institute of Standards and Technology for fellowships, subject to the provisions of section 18 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–1), to support students at institutions of higher learning in computer security. Amounts authorized by this section shall not be subject to the percentage limitation stated in such section 18.

SEC. 11. STUDY OF PUBLIC KEY INFRASTRUCTURE BY THE NATIONAL RESEARCH COUNCIL.

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

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

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

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

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

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

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

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

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

(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary of Commerce $450,000 for fiscal year 2001, to remain available until expended, for carrying out this section.

SEC. 12. PROMOTION OF NATIONAL INFORMATION SECURITY.

The Under Secretary of Commerce for Technology shall—

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

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

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

SEC. 13. ELECTRONIC AUTHENTICATION INFRASTRUCTURE.

(a) ELECTRONIC AUTHENTICATION INFRASTRUCTURE.—

(1) GUIDELINES AND STANDARDS.—Not later than 18 months after the date of the enactment of this Act, the Director, in consultation with industry and appropriate Federal agencies, shall develop electronic authentication infrastructure guidelines and standards for use by Federal agencies to assist those agencies to effectively select and utilize electronic authentication technologies in a manner that is—

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

(B) interoperable, to the maximum extent possible.

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

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

(B) a core set of interoperability specifications for the Federal acquisition of electronic authentication products and services; and

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

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

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

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

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

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

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

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

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

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

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

(e) NATIONAL POLICY PANEL FOR DIGITAL SIGNATURES.—

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

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

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

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

(C) audit procedures for certification authorities.

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

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

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

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

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

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

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

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

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

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

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

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

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

SEC. 14. SOURCE OF AUTHORIZATIONS.

There are authorized to be appropriated to the Secretary of Commerce $7,000,000 for fiscal year 2001 and $8,000,000 for fiscal year 2002, for the National Institute of Standards and Technology to carry out activities authorized by this Act for which funds are not otherwise specifically authorized to be appropriated by this Act.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Wisconsin (Mr. SENSENBRENNER) and the gentleman from Texas (Mr. HALL) each will control 20 minutes.

The Chair recognizes the gentleman from Wisconsin (Mr. SENSENBRENNER).

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. 2413.

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

There was no objection.

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

Mr. Speaker, H.R. 2413 updates the Computer Security Act of 1987 to improve computer security for Federal civilian agencies and the private sector. The Computer Security Act of 1987 gave authority over computer and communications security standards and Federal civilian agencies to NIST. The Computer Security Enhancement Act of 2000 strengthens that authority and directs funds to implement practices and procedures which will ensure that the Federal standards-setting process remains open to public input and analysis. When implemented, the bill will provide guidance and assistance on protection of electronic information to Federal civilian agencies.

Since 1993, the General Accounting Office has issued over 35 reports describing serious information security weaknesses at major Federal agencies. In 1999, the GAO reported that during the previous 2 years serious information security control weaknesses had been reported for most of the Federal agencies. Recently, the GAO gave the Federal Government an overall grade of D minus for its computer security efforts. Specifically, hearings held by the Committee on Science earlier this year identified information security leaks at the Department of Energy and the Federal Aviation Administration that threaten our Nation's safety, security, and economic well-being.

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

1400

The Computer Security Enhancement Act of 2000 addresses these changes, promotes the use of commercially available products, and encourages an open exchange of information between NIST and the private sector, all of which will help facilitate better security for Federal systems.

Finally, the legislation is technology neutral and is careful not to advocate any specific computer security or electronic authentication technology.

Mr. Speaker, while no single piece of legislation can fully protect our Federal civilian computer security systems, H.R. 2413 is a necessary step in the right direction. It has been unanimously supported by the Committee on Science and includes a number of provisions offered by the gentleman from Tennessee (Mr. GORDON); the gentlewoman from Maryland (Mrs. MORELLA), chair of the Subcommittee on Technology; the gentleman from Michigan (Mr. BARCIA), ranking member of that subcommittee; and the gentleman from California (Mr. KUYKENDALL), a member of the Cyber Security Leadership Team of the gentleman from Illinois (Mr. HASTERT).

I urge all my colleagues to support swift passage of this bill today.

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

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

Mr. Speaker, I would first, of course, like to compliment the gentleman from Michigan (Mr. BARCIA) and the gentlewoman from Maryland (Mrs. MORELLA) and the gentleman from Tennessee (Mr. GORDON) and, of course, the chairman, the gentleman from Wisconsin (Chairman SENSENBRENNER), for their very hard work on this question of computer security.

I get asked about that so very much and so very often. This has been an important topic for this committee for 15 years or more and dating back to the committee at the time when Congressman Jack Brooks enacted the very first security computer law dealing with federally owned computers.

H.R. 2413 brings our computer security efforts into the Internet age by working to upgrade the security of unclassified Federal computer systems and networks. The computer world has changed dramatically since we wrote the original Computer Security Act in the mid-1980s. Then we were coping with a new set of problems brought about by the arrival of personal securities and the movement of computer security problems that move beyond the mainframe computers.

Now, with the arrival of the World Wide Web, attacks on government computers are far more difficult to detect and certainly come from anywhere in the world. So effective and coordinated Federal computer security is now more important than it has ever been before.

H.R. 2413 confirms the National Institute of Standards and Technology's lead role in setting policy guidelines and measuring the effectiveness of computer security practices in civilian agencies.

NIST is also authorized to provide guidance and assistance to Federal agencies in the protection of interconnected computer systems and to promote compliance by Federal agencies with the existing computer information security and privacy guidelines and to assist other agencies in responding to unauthorized access to Federal computer systems.

Thanks to the leadership of the gentleman from Tennessee (Mr. GORDON), H.R. 2413 also will permit the Federal Government to advance e-commerce and e-government by providing for secure electronic authentication technologies.

Mr. Speaker, there has never been a time when so much of our lives have been documented by Federal computers. Veterans all across this country have the right to expect their medical records to be secure. Our seniors have to be able to depend on the security of the Social Security Administration's computers. The IRS must be able to protect our tax records from disclosure. Small businesses that deal with the government must have their records protected from potential competitors.

NIST has long been a leader in computer security, and it makes a lot of sense for NIST to share this expertise with other agencies. Therefore, I urge my colleagues to pass this important piece of legislation.

Mr. Speaker, the gentleman from Tennessee (Mr. GORDON), who is the ranking member on the Subcommittee on Space and Aeronautics, has been unbelievably supportive in the drawing and passing and bringing to this stage this piece of legislation.

Mr. Speaker, I yield such time as he may consume to the gentleman from Tennessee (Mr. GORDON).

Mr. GORDON. Mr. Speaker, I rise in support of H.R. 2413.

The gentleman from Wisconsin (Chairman SENSENBRENNER) and the gentleman from Texas (Mr. HALL) have already outlined the provisions of this bill.

I would like to take a couple of minutes to stress two points. First, the provisions of this bill are technologically neutral; and second, the bill would allow for strong private sector input in the development of good Federal computer security and authentication practices.

The bill that we have on the floor today is the result of 2 years of bipartisan work on the Committee on Science. The Committee on Science has held numerous hearings on these provisions, and we have incorporated constructive changes suggested by the industry and the administration.

The resulting legislation strengthens NIST's role in improving the computer security practices at Federal agencies. It also authorizes NIST to advise the agencies as needed on the deployment of electronic authentication technologies. These provisions ensure that the private sector has a strong voice in the development of electronic authentication policies considered by the Federal agencies and that agencies rely on commercially available products and service as much as possible.

The bill also makes clear that any Federal policies on computer security and electronic authentication practices by Federal agencies must be technologically neutral.

I again want to thank the gentleman from Wisconsin (Chairman SENSENBRENNER) for his leadership on this issue and working closely with me on this legislation. We have both been motivated by the importance that we place on the broad issues of electronic security.

In addition, I want to thank Mike Quear and Jeff Grove on the Committee on Science and the staff of the Committee on Commerce on both sides for their work for perfecting this legislation.

This is a good bill representing sound policy. I urge my colleagues to support H.R. 2413.

Mrs. MORELLA. Mr. Speaker, over the last four years, the Technology subcommittee that I chair in the Science Committee has held several hearings on computer security and has reviewed H.R. 2413 in depth. Computer security continues to be an ongoing and challenging problem that demands the attention of the Congress, the Executive Branch, industry, academia, and the public.

The explosive growth in Electronic Commerce highlights the nation's ever increasing dependence upon the secure and reliable operation of our computer systems. Computer security, therefore, has a vital influence on our economic health and our nation's security, and that is why it is important that we pass H.R. 2413 here today.

H.R. 2413 authorizes $9 million in FY 2001 and $9.5 million in FY 2002 to the National Institute of Standards and Technology to: Promote the use of commercially available off-the-shelf security products by Federal agencies, an initiative strongly supported by the Information Technology Association of America and others; Increase privacy protection by giving an independent advisory board more responsibility and resources to review NIST's computer security efforts and make recommendations; Support the development of well trained workforce by creating a fellowship program in the field of computer security; Study the efforts of the Federal government to develop a secure, interoperable electronic infrastructure; and finally,—Establish an expert review team to assist agencies to identify and fix existing information security vulnerabilities.

I am proud of the important work NIST is doing in the area of computer security, and I am pleased H.R. 2413 provides additional resources and tools to assist in its efforts.

Located in Gaithersburg, Maryland, NIST plays a critical role to improve computer security for the Federal Government and the private sector. Under NIST's statutory federal responsibilities, it works to develop standards and guidelines for agencies to help protect their sensitive unclassified information systems.

Additionally, NIST works with the information technology (IT) industry and IT users in the private sector on computer security in support of its

broad mission to strengthen the U.S. economy, and especially to improve the competitiveness of the U.S. information technology industry. In conducting its computer security efforts, NIST works closely with industry, Federal agencies, testing organizations, standards groups, academia, and private sector users.

Specifically, NIST works to improve the awareness of the need for computer security and conducts cutting-edge research on new technologies and their security implications and vulnerabilities. NIST works to develop security standards and specifications to help users specify security needs in their procurements and establish minimum-security requirements for Federal systems.

NIST develops and managers security-testing programs, in cooperation with private sector testing laboratories, to enable user to have confidence that a product meets a security specification. Finally, NIST produces security guidance to promote security planning, and secure system operations and administration.

I have already mentioned NIST's important role in standards development. NIST has long been active in developing Federal cryptographic standards and working in cooperation with private sector voluntary standards organizations in this area. Recently, NIST facilitated the worldwide competition to develop a new encryption technique that can be used to protect computerized information, know as the Advanced Encryption Standard (AES), which will serve 21st century security needs.

Another aspect of NIST's standards activities concerns Public Key and Key Management Infrastructures. The use of cryptographic services across networks requires the use of ''certificates'' that bind cryptographic keys and other security information to specific users or entities in the network. NIST has been actively involved in working with industry and the Federal government to promote the security and interoperability of such infrastures.

Mr. Speaker, a wide array of technology organizations and the Administration have recognized the need for H.R. 2413 and to protect our nation's information technology security. I urge my colleagues to stand with these organizations and myself to take this important step towards securing our computer data and resources from malicious attack. I urge passage of H.R. 2413.

Ms. JACKSON-LEE of Texas. Mr. Speaker, I rise in strong support for H.R. 2413, the Computer Security Enhancement Act of 2000. This bill reinforces the role of the National Institute of Standards and Technology (NIST) in ensuring the security and privacy of federal civilian computer systems, and promotes the use of technology solutions developed by the private sector. The measure affirms NIST's role as the lead agency for creating and maintaining standards for federal computer security and emphasizes the need for protecting sensitive information in federal databases and on publicly accessible government Web sites. The committee states that NIST should focus on security issues that have emerged with the rapid changes in computer technology since passage of the Computer Security Act of 1987.

The bill authorizes $7 million in FY 2001, and $8 million in FY 2002 for NIST to carry out the measure, not including funds otherwise specifically authorized.

This legislation comes in response to a 1999 General Accounting Office (GAO) report that stated that, during the previous two years, serious information security control weaknesses had been reported for most federal agencies, and GAO recently gave the federal government an overall grade of ''D-minus'' for its computer security efforts.

The Computer Security Act of 1987 (P.L. 100–235) gave authority over computer and communication security standards in federal civilian agencies to the National Institute of Standards and Technology (NIST). However, the Science Committee notes that there have been dramatic changes in computer technology since the 1987 Act, citing the proliferation of networked systems, the Internet and Web access.

The bill authorizes NIST to provide guidance and assistance—including risk identification—to Federal agencies in the protection of information technology infrastructure (except for national security systems); provide information on existing security and privacy guidelines to promote compliance by Federal agencies; and consult with agencies on incidences of unauthorized access to Federal computer systems. The bill instructs NIST to develop measures to assess the effectiveness of agencies' privacy programs, perform evaluations and promote accreditation procedures for agency information security programs. The bill also directs NISt to report annually to Congress on its evaluations of federal computer systems, the use of commercially available security products by agencies, evaluations planned for the next year and any recommendations resulting from past evaluations.

The bill requires NIST to work with the Computer System Security and Privacy Advisory Board in setting standards and guidelines for the security of federal computer systems and to include the board's recommendations in Commerce Department reviews of proposed standards, guidelines and regulations. The measure authorizes $1 million in each of FY 2001 and FY 2002 for the board to hold public meetings and publish reports and other relevant information on emerging computer security and cryptology issues. the board, made up of representatives from industry, federal agencies and outside experts, would report directly to the science committees in the House and Senate.

The measure prohibits NIST from creating or enforcing any standards or policies relating to computer systems outside the federal government.

I believe that this is an important step to take in our effort to encourage computer network security in the federal workplace.

However, I would advise that it is also important that the federal government develops and maintain an adequate supply of computer security professionals. We must be sure that those who are entrusted with the network security of our nation's interconnected computers are dedicated and well trained information and network security experts.

Far too often those who are assigned network administrative functions, must share that responsibility among other assigned task, which might take precedence over their computer system responsibilities. The computer system is not deemed a priority unless access to files and informational resources are denied, then the systems specialist is expected to respond quickly to address the problem and restore service. The responsibility of network security is to maintain the routine maintenance of the system, which is vital to the smooth overall functioning of a computer system.

Mr. HALL of Texas. Mr. Speaker, 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. HANSEN). 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. 2413, as amended.

The question was taken; and the Speaker pro tempore announced that the ayes appeared to have it.

Mr. HALL of Texas. 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 8 of rule XX and the Chair's prior announcement, further proceedings on this motion will be postponed.

The point of no quorum is considered withdrawn.

NATIONAL SCIENCE EDUCATION ACT

Mr. SENSENBRENNER. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 4271) to establish and expand programs relating to science, mathematics, engineering, and technology education, and for other purposes, as amended.

The Clerk read as follows:

H.R. 4271

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 ''National Science Education Act''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) As concluded in the report of the Committee on Science of the House of Representatives, ''Unlocking Our Future Toward a New National Science Policy'', which was adopted by the House of Representatives, the United States must maintain and improve its preeminent position in science and technology in order to advance human understanding of the universe and all it contains, and to improve the lives, health, and freedoms of all people.

(2) It is estimated that more than half of the economic growth of the United States today results directly from research and development in science and technology. The most fundamental research is responsible for investigating our perceived universe, to extend our observations to the outer limits of what our minds and methods can achieve,