

for Federal agencies by requiring NIST to promote the Federal use of off-the-shelf products for meeting civilian agency computer security needs.

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

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

4. Clarifies that NIST standards and guidelines are to be used for the acquisition of security technologies for the Federal Government and are not intended as restrictions on the production or use of encryption by the private sector.

5. Addresses the shortage of university students studying computer security. Of the 5,500 PhDs in Computer science awarded over the last five years in Canada and the U.S., only 16 were in fields related to computer security. To help address such shortfalls, the bill establishes a new computer science fellowship program for graduate and undergraduate students studying computer security; and

6. Requires the National Research Council to conduct a study to assess the desirability of creating public key infrastructures. The study will also address advances in technology required for public key in technology required for public key infrastructure.

7. Establishes a national panel for the purpose of exploring all relevant factors associated with the development of a national digital signature infrastructure based on uniform standards and of developing model practices and standards associated with certification authorities.

All these measures are intended to accomplish two goals. First, assist NIST in meeting the ever-increasing computer security needs of Federal civilian agencies. Second, to allow the Federal Government, through NIST, to harness the ingenuity of the private sector to help address its computer security needs.

Since the passage of the Computer Security Act, the networking revolution has improved the ability of Federal agencies to process and transfer data. It has also made that same data more vulnerable to corruption and theft.

The General Accounting Office (GAO) has highlighted computer security as a government-wide, high-risk issue. GAO specifically identified the lack of adequate security for Federal civilian computer systems as a significant problem. Since June of 1993, the General Accounting Office (GAO) has issued over 30 reports detailing serious information security weaknesses at 24 of our largest Federal agencies.

The Science Committee has held seven hearings on computer security since I became Chairman in 1997. During the hearings, Mem-

bers of the Science Committee heard from some of the most respected experts in the field. They all agreed that the Federal Government must do more to secure the sensitive electronic data it possesses.

The Federal Government is not alone in its need to secure electronic information. The corruption of electronic data threatens every sector of our economy. The market for high-quality computer security products is enormous, and the U.S. software and hardware industries are responding. The passage of this legislation will enable the Federal Government, through NIST, to benefit from these technological advances.

I look forward to working with all interested parties to advance the Computer Security Enhancement Act of 1999. In my estimation, it is a good bill, and I am hopeful we can move it through the legislative process in short order.

THE COMPUTER SECURITY ENHANCEMENT ACT OF 1999

HON. BART GORDON

OF TENNESSEE

IN THE HOUSE OF REPRESENTATIVES

Thursday, July 1, 1999

Mr. GORDON. Mr. Speaker, today, I am pleased to join Chairman SENSENBRENNER in introducing the Computer Security Enhancement Act of 1999. I was an original co-sponsor of similar legislation in the 105th Congress. The measure follows a stream of attacks just this past week on government Web sites including the Senate, White House, the National Oceanic Atmospheric Administration's severe weather warning site, the Defense Department and the FBI's National Infrastructure Protection Center, whose very purpose is to protect federal sites from such attacks.

The Computer Security Enhancement Act of 1999 will encourage the use of computer security products, both by federal agencies and the private sector, which in turn will support the new electronic economy. I am convinced that we must have trustworthy and secure electronic network systems to foster the growth of electronic commerce. This legislation builds upon the successful track record of the National Institute of Standards and Technology (NIST) in working with industry and other federal agencies to develop a consensus on the necessary standards and protocols required to support electronic commerce.

Chairman SENSENBRENNER has already outlined the provisions of this bill. However, I would like to take a few minutes to explain provisions I added to this legislation that are based on H.R. 1572, the Digital Signature Act of 1999, which I introduced with the support of Chairman SENSENBRENNER on 27 April 1999 to complement last year's Government Paperwork Elimination Act. When I introduced H.R. 1572, I stated that it was a work in progress. Section 13 of the Computer Security Enhancement Act, which we are introducing today, is the result of discussions I have had with industry and federal agencies.

As a result of these discussions, the general provisions in H.R. 1572 have been re-drafted to include all electronic authentication techniques. Section 13 requires NIST, working

with industry, to develop minimum technical standards and guidelines for Federal agencies to follow when deploying any electronic authentication technologies. In addition, Section 13 authorizes the Undersecretary of Commerce for Technology to establish a National Policy Panel for Digital Signatures to explore the factors associated with the development of a National Digital Signature Infrastructure based on uniform model guidelines and standards to enable the widespread utilization of digital signatures in the private sector.

I want to highlight that these provisions are technology neutral. Rather they encourage federal agencies to use uniform guidelines and criteria in deploying electronic authentication technologies and to ensure that their systems are interoperable. The provisions also encourage agencies to use commercial off-the-shelf software (COTS) whenever possible to meet their needs. None of these provisions give the Federal government the authority to establish standards or procedures for the private sector.

The use of electronic authentication technologies are critical for the continued growth and security of electronic transactions on the Internet. With the rapid growth of the Internet we have lost the ability to actually "know" who we are communicating with is who they say they are. In order to exchange sensitive documents or to do business transactions with confidence it is important that electronic authentication systems are used that both uniquely identify both the sender and/or the recipient and verify that the information exchanged has not been altered in transit. Electronic authentication is as much of a computer security issue as having good firewalls, strong encryption, and virus scanners.

I want to stress the underlying principle of the Computer Security Enhancement Act of 1999 is that it recognizes that government and private sector computer security needs are similar. Hopefully the result will be greater security and lower cost for everyone as we increasingly move towards an electronic economy.

The bill we are introducing today is the result of close bipartisan cooperation and it has been a pleasure working with Chairman SENSENBRENNER on this legislation.

I urge my colleagues to support the Computer Security Enhancement Act of 1999.

EDUCATIONAL TECHNOLOGY UTILIZATION EXTENSION ASSISTANCE ACT

HON. JAMES A. BARCIA

OF MICHIGAN

IN THE HOUSE OF REPRESENTATIVES

Thursday, July 1, 1999

Mr. BARCIA. Mr. Speaker, I am pleased to introduce, along with my friend from Oregon, Mr. Wu, the Educational Technology Utilization Extension Assistance Act. This bill directs the National Science Foundation to work with the Department of Education and the National Institute of Standards and Technology to create educational technology extension centers based at undergraduate institutions. The focus of these centers is to advise and assist local K-12 schools to better utilize and integrate