H.R. 2413, THE COMPUTER SECURITY ENHANCEMENT ACT OF 1999

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY

OF THE

COMMITTEE ON SCIENCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

SEPTEMBER 30, 1999

Serial No. 106–45

Printed for the use of the Committee on Science

U.S. GOVERNMENT PRINTING OFFICE
61–162 WASHINGTON : 2000

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-060065-0

COMMITTEE ON SCIENCE

F. JAMES SENSENBRENNER, Jr., *Chairman*

SHERWOOD L. BOEHLERT, New York
LAMAR SMITH, Texas
CONSTANCE A. MORELLA, Maryland
CURT WELDON, Pennsylvania
DANA ROHRABACHER, California
JOE BARTON, Texas
KEN CALVERT, California
NICK SMITH, Michigan
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan
DAVE WELDON, Florida
GIL GUTKNECHT, Minnesota
THOMAS W. EWING, Illinois
CHRIS CANNON, Utah
KEVIN BRADY, Texas
MERRILL COOK, Utah
GEORGE R. NETHERCUTT, Jr., Washington
FRANK D. LUCAS, Oklahoma
MARK GREEN, Wisconsin
STEVEN T. KUYKENDALL, California
GARY G. MILLER, California
JUDY BIGGERT, Illinois
MARSHALL "MARK" SANFORD, South Carolina
JACK METCALF, Washington

RALPH M. HALL, Texas
BART GORDON, Tennessee
JERRY F. COSTELLO, Illinois
JAMES A. BARCIA, Michigan
EDDIE BERNICE JOHNSON, Texas
LYNN C. WOOLSEY, California
LYNN N. RIVERS, Michigan
ZOE LOFGREN, California
MICHAEL F. DOYLE, Pennsylvania
SHEILA JACKSON-LEE, Texas
DEBBIE STABENOW, Michigan
BOB ETHERIDGE, North Carolina
NICK LAMPSON, Texas
JOHN B. LARSON, Connecticut
MARK UDALL, Colorado
DAVID WU, Oregon
ANTHONY D. WEINER, New York
MICHAEL E. CAPUANO, Massachusetts
BRIAN BAIRD, Washington
JOSEPH M. HOEFFEL, Pennsylvania
DENNIS MOORE, Kansas
Vacancy

CONTENTS

September 30, 1999

Witnesses

Appendix: H.R. 2413, Statements, and Testimony Submitted for the Record

H.R. 2413, THE COMPUTER SECURITY ENHANCEMENT ACT OF 1999

THURSDAY, SEPTEMBER 30, 1999

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

The Subcommittee met, pursuant to notice, at 1:30 p.m., in Room 2318, Rayburn House Office Building, Hon. Constance Morella [Chairwoman of the Subcommittee] presiding.

Chairwoman MORELLA [presiding]. I'm pleased to call to order this afternoon's Technology Subcommittee hearing.

You may have heard me in the past compare our Nation's lack of adequate information security to the year 2000 computer problem. Despite the money, manpower or womanpower, and management priority we've exerted on the Y2K problem, I believe the lack of adequate computer security protection in our federal agencies has the potential to dwarf the millennium bug in scope and magnitude.

Through the cooperative efforts of Congress, the private sector, and the media, everyone is now aware of Y2K, but few still recognize the threat and vulnerabilities associated with the lack of computer security. And with Y2K, we all know the deadline—January 1, 2000—and federal agencies are collectively gearing up to meet the challenges that may occur on that date.

Information security attacks or cyber attacks, however, can happen at any time—today and throughout the next century—and do not provide federal agencies with the luxury of collectively preparing for these attacks, that is, unless we begin now to begin the process of laying the foundation for a coordinated federal effort to guard our information technology systems from hackers or those with nefarious intent.

This is an important issue. It is a clear priority for the Technology Subcommittee. We've already held two hearings this year exploring computer security. In April, we discussed the impact of the Melissa computer virus and other evolving threats to computer and information security. In June, in the face of several well-publicized cyber attacks, we met to review the security of federal agency web sites.

At these hearings, we heard a constant theme. Most federal agencies are simply not doing enough to protect their critical information systems from attacks and corruption. The result of these attacks to a system can be a mere nuisance akin to vandalism or it can be catastrophic and cripple a system that is essential to the agency's mission.

Obviously, securing electronic information is not solely a federal concern. The corruption of electronic data has the potential to also threaten every sector of our economy.

Today we have assembled a distinguished panel of experts to discuss H.R. 2413, the Computer Security Enhancement Act of 1999, a bill that would provide an important first step in our goal of strengthening information technology protection. The legislation strengthens the National Institute of Standards and Technology's historic role in computer security that was established by the Computer Security Act of 1987.

The bill updates the act, gives NIST the tools it needs to ensure that appropriate attention and effort is concentrated on securing our federal information technology infrastructure. Specifically, the bill would require NIST to promote the acquisition of off-the-shelf products for meeting civilian agency computer security needs. This measure should reduce the cost and improve the availability of computer security technologies for federal agencies.

Secondly, it would increase the input of the independent Computer Systems Security and Privacy Advisory Board into NIST's decisionmaking 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.

Thirdly, it would clarify 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.

Fourthly, it would establish a new NIST Computer Science Fellowship Program for graduate and undergraduate students studying computer security, something we very badly need.

And, finally, it would establish a national policy panel to explore the infrastructure needs for a national digital signature system for electronic authentication.

In the past Congress, the bill passed the House. It was cleared by a Senate committee without opposition or amendment, but it was unable to reach the Senate Floor before the 105th Congress adjourned. While no single piece of legislation can fully protect our federal civilian computer systems, H.R. 2413 is a necessary step in the right direction.

I look forward to working with my colleagues, today's witnesses, and all the interested parties to enact into law this important legislation.

And, finally, I want to point out that I share the same goal as my Committee colleague, the gentleman from Tennessee, Mr. Gordon, to create an interoperable digital signature infrastructure in support of all electronic transactions. The provisions he has added to H.R. 2413 significantly improve the legislation, respond to a suggestion made by a number of my constituent companies, and would allow for greater convenience and service for those that do business with the Federal Government.

And, so now it is my pleasure to recognize the distinguished Ranking Member of this Technology Subcommittee, Mr. Barcia.

Mr. BARCIA. Thank you, Chairwoman Morella, and I want to thank you for this timely hearing on this very important legislation and say what a privilege it is to serve as the Ranking Member on this Subcommittee. Not only are you one of the most bipartisan and fair Chairs, but also one of the most ambitious in terms of the work that we do in this Subcommittee, and I think this is a very important hearing today, and thank you for calling it.

Chairwoman MORELLA. I hope the record will show that. Thank you.

Mr. BARCIA. Good afternoon. I want to join Chairwoman Morella in welcoming our distinguished panel to this afternoon's hearing on H.R. 2413, the Computer Security Enhancement Act of 1999.

This is, as the Chairwoman mentioned, the third hearing on this subject of computer security held by the Subcommittee this year. Our last hearing focused on the poor security practices of many federal agencies. At that hearing, our witnesses identified a number of the impediments that prevent federal agencies from implementing better computer security practices, such as the fact that there is no centralized focal point to advise them on good computer security practices or to ensure that computer security practices are properly implemented.

When the Science Committee developed the Computer Security Act 12 years ago, it was our hope that NIST could serve this role. Although NIST's Computer Systems Security and Privacy Advisory Board has not made specific recommendations on changing the Computer Security Act, the board has made a number of recommendations to NIST on how to fully implement the act.

First and foremost, the board has recommended that NIST elevate its commitment to implementing the act by increasing its assistance to civilian federal agencies. The board listed acting as a central repository within the Federal Government to advise on the selection, integration, and use of products and procedures for securing non-classified systems and providing a computer systems security assessment capability for civilian federal agencies as high priority items.

The board also urged NIST to maintain a repository and act as a clearinghouse for information, techniques, guidelines, and consultation to weight proper use of security features available in Government-used, commercial, off-the-shelf software. In a recent letter to Secretary Daley, the board stressed the need for aggressive executive leadership. I support the board's belief that NIST should take a stronger role in computer security issues.

The provisions of H.R. 2413 are entirely consistent with recommendations made by NIST's Private Sector Advisory Board. I would also stress the provisions offered by my good friend and distinguished colleague Bart Gordon are consistent with the vision that the Computer Systems Security and Privacy Advisory Board has for NIST. NIST, as the only federal agency which works closely with the private sector in developing standards, should serve a strong advisory role in the deployment of computer security related technologies of which electronic authentication technologies are a very important component.

I want to thank our witnesses for appearing before us today. I hope that they will continue to work with the Subcommittee to develop a bill that will improve the security of federal computer systems and improve the deployment of electronic authentication.

Thank you very much, Madam Chair, and I'll close my opening remarks.

Chairwoman MORELLA. Thank you, Mr. Barcia.

I'm now pleased to recognize Mr. Gordon from the great State of Tennessee where I guess someone is going to be redirecting a campaign from.

Mr. GORDON. Thank you, Chairwoman Morella and Ranking Member Barcia, for calling this hearing, and I want to welcome you and welcome our witnesses.

I was an original cosponsor of similar legislation in the last Congress, and I am pleased to be a cosponsor of this legislation.

Many of the provisions of H.R. 2413 are the same as passed the House in the 105th Congress. I would like to take a few minutes to talk about provisions that were added to the legislation.

In April, Chairman Sensenbrenner and I introduced H.R. 1572, the Digital Signature Act of 1999. At that time, I stressed that this was a work in progress. Section 13 of the Computer Securities Enhancement Act of 1999 reflects that ongoing work, and it's a result of discussions with industry, NIST, and the Department of Commerce, and I want to thank my staff for all the work they have put in bringing these folks together to try to get our best information.

The most significant change from H.R. 1572 is that the provisions in this bill have been expanded to include all electronic authentication technologies. This change was the result of suggestions made by the Department of Commerce. It's my belief that consistent with the Government Paperwork Elimination Act, federal agencies could serve as a model of such technologies how they could be effective in implementing under section 13 in H.R. 2413 and requires NIST, working with industry, to develop minimum technical guidelines to assist federal agencies deploying electronic authentication systems.

These guidelines would include technical security requirements when operating and maintaining electronic authentication technologies, interoperability considerations for agencies to refer to when selecting electronic authentication products and services, and validation criterion for agencies to use when purchasing commercial electronic authentication products and services. This will also help the private sector develop products and services to meet Government needs.

I'm not alone in my concerns about the need to help federal agencies effectively deploy electronic signatures technologies. In a Federal Technology Week article, Tony Trinkle, Director of Electronic Services at the Social Security Administration, said of H.R. 1572, "The bill moves the debate about standards in the right direction establishing at a time—especially at a time when agencies are trying to comply with the Government Paperwork Elimination Act passed last year."

And I would like to clarify some confusion that exists in the wording of section 13. It was never my intent that NIST develop standards in the general accepted sense of the word. NIST activities would be limited to guidelines and best practices. It is my intention to modify the language to ensure that there is no confusion on this point.

And I want to stress the underlying principles of the Computer Securities Enhancement Act of 1999 is that it recognizes that Government and private sector computer security needs are similar. In drafting the electronic authentication provisions, I tried to ensure that the private sector would have a strong voice in development of any guidelines used by the agencies.

I would also add that both the European Commission and Canada are already working on implementing national digital signature infrastructures to facilitate the widespread use of electronic signatures in their computers.

This hearing is an opportunity to begin a discussion on how to develop policies for federal agencies which will allow them to effectively and efficiently deploy electronic signature technologies and improve the security of their computer systems. As a recent spat of widespread break-ins highlights, the GAO report confirms we have a long way to go.

I look forward to working with the panelists to strengthen this bill and thank them for appearing before this Subcommittee today.

Chairwoman MORELLA. Thank you, Mr. Gordon. Thanks for your work on the bill too, and I am pleased to recognize Ms. Rivers from Michigan. You are always very punctual being here.

And, Mr. Baird, from the great State of Washington.

Okay, great. All right.

Then moving ahead, as I mentioned earlier, we're fortunate to have a distinguished panel of experts with us this afternoon to discuss this important issue. People are no strangers to this Committee by and large, and I welcome them, and thank you for being here.

First, Mr. Ray Kammer, the Director of the National Institute of Standards and Technology, will testify. Mr. Kammer has appeared before this Committee so many times during his 30-year career with the Department of Commerce that we cannot even record the total number with accuracy.

Next, we have Mr. Keith Rhodes, the Director of Computer and Information Technology Assessment with the General Accounting Offices, Accounting and Information Management Division, and this is Mr. Rhodes' fourth appearance before this panel this year. I very much appreciate the important work that Mr. Rhodes and his colleagues at GAO do in support of this Subcommittee's efforts.

Thirdly, we have Mr. Harris Miller, who is the President of Information Technology Association of America. Mr. Miller was recently recognized by Washingtonian magazine as one of the most influential association presidents in America. Obviously he's no stranger to this Subcommittee, having appeared before us numerous times regarding the year 2000 computer problem; one of the first witnesses, as a matter of fact, I think that we had like 3½ years ago, more than that.

Lastly, we'll hear from Professor George Trubow of the John Marshall Law School where he directs the Center for Information Technology and Privacy Law in addition to his teaching responsibilities. Professor Trubow is a member of the Computer Systems

Security and Privacy Advisory Board, which advises NIST on computer security and privacy matters.

Again, I want to thank all the witnesses for being with us today. I look forward to hearing the testimony.

And, finally, I want to point out that the Subcommittee will receive testimony for the record from Mr. Charles Talley, the Director of the Information Engineering Center at the OAO Corporation in Greenbelt, Maryland. Mr. Talley has a distinguished 33-year career in information technology. We're fortunate that he has shared his comments in support of H.R. 2413 with us. His testimony, just as the testimony of all of you, in its entirety, will be included in the record and posted on our web site.

Chairwoman MORELLA. The tradition for all of the subcommittees in the full Science Committee is that we swear in the people who testify. If you'd stand, raise your right hand.

Do you solemnly swear that the testimony you are about to give is the truth, the whole truth, and nothing but the truth?

Mr. KAMMER. I do.

Mr. RHODES. I do.

Mr. MILLER. I do.

Mr. TRUBOW. I do.

The record shows an affirmative response, and we'll start off right away with the Honorable Raymond Kammer, Director of NIST.

STATEMENT OF RAYMOND KAMMER, DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY; ACCOMPANIED BY KEITH RHODES, DIRECTOR, TECHNOLOGY ASSESSMENT, UNITED STATES GENERAL ACCOUNTING OFFICE; HARRIS MILLER, PRESIDENT, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA; AND GEORGE B. TRUBOW, DIRECTOR, CENTER FOR INFORMATION TECHNOLOGY & PRIVACY LAW, THE JOHN MARSHALL LAW SCHOOL

STATEMENT OF RAYMOND KAMMER

Mr. KAMMER. Madam Chairwoman, Mr. Barcia, Mr. Gordon, Ms. Rivers, Mr. Baird, good afternoon to all of you. Thank you for inviting me here today to testify on H.R. 2413, the Computer Security Enhancement Act of 1999.

NIST, of course, is part of the Technology Administration, which is part of the Department of Commerce, and within NIST, NIST Computer Security Division in our Information Technology lab is the focal point for our security program.

Our program focuses on a few key areas: cryptographic standards and guidelines, public key infrastructure, security research, agency assistance, and the national information assurance partnership, which is jointly managed by NIST and NSA, and its focus is to increase the availability of quality information technology security products.

I'd like to bring to the Committee's attention the President's very recent request for an additional $39 million in Fiscal Year 2000 for initiatives proposed to protect critical infrastructure in both the Government and the private sector. A total of $5 million of this request is proposed for NIST, and this critical infrastructure protection proposal would establish an expert review team at NIST which would assist other Government agencies in adhering to federal computer security requirements.

Of the $5 million requested, $2 million is for a 15-member team that would work at NIST to be responsible for helping agencies identify vulnerabilities, planned security systems, and implement their plans. The remaining $3 million would represent—would establish an operational fund which would support projects that would benefit the general Federal agencies. Projects might include independent vulnerability assessments, computer intrusion drills, emergency funds to cover security fixes that weren't anticipated, and the like.

My view is that the Computer Security Act of 1987 remains an appropriate framework for addressing federal computer security issues, but technology changes and so must we all. And in my view, the actions of the Committee and the authors of this bill is a very appropriate way to address some of the critical issues that have developed since the last time this bill was drafted.

I'd like now to note a few topics where I would prize having further conversation with the Committee on the exact wording of some sections of the bill. First, the bill poses in section four to assign NIST responsibility to coordinate Federal response efforts related to unauthorized access to Federal computing systems, and I think that's an appropriate assignment. But my thought is that NIST can coordinate, they can assist people, but we need to make sure that the agencies realize that they remain—they have the primary responsibility for maintaining the security of their own agencies. Only they can decide how valuable the data is that's protected and, therefore, how much resource should go on it.

Section five would require NIST to emphasize the development of technology-neutral policy guidelines for computer security practices by the Federal Government, and the policies can be neutral, but technology implementation itself requires choices that are made to the exclusion of other choices. It is if you work on one technology, you're not working on another one. And we hope that this section not be misinterpreted to preclude the kind of appropriate technical activities where we join with other agencies and the private sector to advance the ball on security practices.

Section six, as currently written, would require NIST to solicit recommendations of the Computer Systems Security Privacy Advisory Board before submitting a proposed Federal standard to the Secretary and to submit the board's recommendation along with ours. I worry that perhaps the board is not always going to be able to respond as rapidly as we may need to respond. And, also, the possibility would exist if the board didn't decline to comment on a particular proposal, that would effectively stymie it under this regime. Professor Trubow, representing the board, actually, has proposed a solution in his testimony that I think would work great.

Section seven has a limitation on participating and requiring encryption standards that would prohibit NIST from promulgating, enforcing, or otherwise adopting standards for the Federal establishment of encryption standards that were required in other than Federal systems. And, again, we have no need, desire, or right to impose on anybody, even including the Federal Government; we usually provide guidelines.

But, currently, DES is most widely used by the banking industry. As the Committee knows, I plan to announce a replacement or perhaps replacements for DES next summer. When I do, my expectation is that the banking industry will be eager to replace DES with the advanced encryption standard. I'd like to be able to be sure I can work with them to make sure that that's easily and efficiently done and works to their advantage as well as the general public's.

Representative Gordon mentioned that he was concerned now that section 13 could be interpreted to require standards when indeed guidelines and best practices were what he had in mind. I had a similar comment in my testimony, and we're eager to work with you to get to the objective that you stated, Mr. Gordon.

So, with that, thank you to the Committee for inviting me, and I'll be happy to answer questions at the appropriate time.

[The statement of Mr. Kammer follows:]

Statement of
Raymond G. Kammer
Director

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

before the

House Science Committee's
Subcommittee on Technology

September 30, 1999

Good morning. Thank you, Madame Chairwoman, for inviting me here today to testify on H.R. 2413, the Computer Security Enhancement Act of 1999. I am Ray Kammer, Director of the National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce's Technology Administration. You may recall that I testified before you in April on the Melissa computer virus and on Web security in June. It is a pleasure to be back again. Your continued attention to computer security issues is most appropriate, given our growing dependence upon technology for more and more of the business of our daily lives -- both personal and professional. Today I would like to start by briefly reviewing our computer security responsibilities and program. Then I propose to share with you our views on how the Computer Security Enhancement Act of 1999 will strengthen our program and the security of Federal agencies.

NIST'S COMPUTER SECURITY RESPONSIBILITIES

In the area of computer security, NIST has specific statutory responsibilities for developing standards and guidelines to assist Federal agencies in the protection of sensitive unclassified systems. This is in addition to our broad mission of strengthening the U.S. economy -- including improving the competitiveness of America's information technology (IT) industry. In support of this mission, we conduct standards and technology work to help industry produce more secure, yet cost-effective, products, which we believe will be more competitive in the marketplace. Having more secure products available in the marketplace will, of course, also benefit agencies, since they will be using commercial products to secure their systems.

NIST's Computer Security Division in our Information Technology Laboratory (ITL) is the focal point of our security program. Our program focuses on a few key areas: cryptographic standards and guidelines; public key infrastructure; security research; agency assistance and the National Information Assurance Partnership, which is jointly managed by NIST and the National Security Agency to focus on increasing the number and quality of IT security products. A few examples of our work include our efforts on the Advanced Encryption Standard (AES), and on emerging technologies for protecting Internet security and interoperability to support public key infrastructure technology. Approximately $5 million of direct Congressional funding supports both the Federal and industry computer security responsibilities that I spoke of earlier. In addition, we work with Federal agencies, receiving approximately $3 million in outside agency funding to provide technical assistance on particular projects.

Our Federal responsibilities, as assigned in the Computer Security Act (P.L. 100-235), focus on "developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems." For example, NIST has recently published updated guidelines for training employees in computer security. NIST also sets security cryptographic standards for Federal agencies. We support these standards by operating a conformance testing program that enables agencies to have confidence that cryptographic security products meet government standards. NIST's standards, guidelines, and other products and services assist agencies in implementing their computer security programs as required by Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Resources." Detailed information about our work products is available at our Computer Security Resource Clearinghouse (http://csrc.nist.gov). Among other publications, NIST's Information Technology

Laboratory publishes bulletins to provide timely, up-to-date information on significant security issues. We encourage all agencies to make use of the many resources available through our clearinghouse.

NIST also works closely with Federal officials and organizations with related computer security responsibilities. We are engaged with the Chief Information Officers' Security Committee and officials of the Critical Information Assurance Office to offer our perspective and expertise to their efforts. We work closely with the Federal Public Key Infrastructure Steering Committee under the Government Information Technology Services Board, and chair their Technical Working Group to promote the use of public key technology within Federal agencies. We host and chair an informal information sharing group of Federal computer security program managers, to assist in information sharing among agencies and reduce the potential for costly duplication of work. We work closely with computer security educators to improve the quality of security training to Federal agencies. We are engaged with those organizations responsible for the security of classified systems to identify when their technology and solutions may be cost-effectively adapted to protect unclassified systems. NIST supports and serves as Secretariat for the Computer System Security and Privacy Advisory Board, which assists us by providing advice from an outside perspective. And, finally, we work closely with the Office of Management and Budget on issues regarding Federal implementation of OMB Circular A-130, Appendix III, which provides a consistent framework for security among all Federal agencies.

I would also like to mention the President's very recent request for an additional $39 million in FY 2000 for initiatives proposed to protect critical infrastructure in both the Government and the private sector that is necessary to ensure our national security, national economic security, and public health and safety. A total of $5 million from this request will be provided to NIST. This Critical Infrastructure Protection (CIP) proposal will establish an Expert Review Team at NIST, which will assist Government-wide agencies in adhering to Federal computer security requirements. We will consult with the Office of Management and Budget and the National Security Counsel on the team's plan to protect and enhance computer security for Federal agencies.

Of the additional $5 million requested, $2 million will fund a 15 member team responsible for helping agencies identify vulnerabilities, plan secure systems, and implement CIP plans. The remaining $3 million will establish an operational fund at NIST for computer security projects among federal agencies. Such projects would include independent vulnerability assessments, computer intrusion drill, and emergency funds to cover security fixes for systems identified to have unacceptable risks.

THE COMPUTER SECURITY ENHANCEMENT ACT OF 1999: STRENGTHENING AND UPDATING THE COMPUTER SECURITY ACT OF 1987

Two years ago, at the tenth anniversary of the Computer Security Act of 1987, the Computer System Security and Privacy Advisory Board met to discuss whether changes were needed to be made to the Act. The Board solicited views from the private and public sectors. The Board did not recommend any changes to the Act -- a fact discussed with you in prior testimony. The Board's position supports my view that the Act remains an appropriate overall framework for addressing Federal computer security issues. That said, it is also the case that technology continues to develop, which is reflected in the broad intent and important specific updates proposed in the Computer Security Enhancement Act of 1999, upon which we are focused today.

I would like to commend the Committee and the authors of this bill for recognizing the importance of securing sensitive Federal systems and proposing steps to update the Act to reflect advances in technology since its passage. Introduction of the bill has already served to remind agencies of their responsibilities to provide appropriate, cost-effective security for their sensitive information in computer systems.

In a variety of respects, the bill is consistent with and reinforces our current responsibilities for leadership in developing standards and guidelines for the security of Federal systems. It also reinforces our work with the private sector in developing and implementing voluntary standards, guidelines, and conformity assessment practices and techniques. The bill recognizes the importance that authentication technologies will play in securing our Federal government systems and networks. It also highlights the importance of securing publicly accessible systems, promotes our work with industry to improve the security of commercial products, and further stresses the need for Federal agencies to use these products to meet their security requirements.

We are pleased to see the bill's positive focus on training to improve the number and quality of computer security experts by establishing a computer security fellowship program. NIST, in its continuing efforts to recruit, train, and retain top-notch computer security experts, is keenly aware of the need for increased attention to IT security research and training individuals to conduct research and develop the standards and guidelines needed by Federal agencies. Federal Government support is critical, and we strongly support your efforts to provide for these fellowships. In carrying out this activity, we would consult with the National Science Foundation, which has the lead in graduate study and training in this area.

The bill will help us promote the use of security technologies to secure the nation's information infrastructure by increasing public awareness of information security threats. In many ways, this bill will help us to do a better job of promoting security and strengthening our nation's protection against emerging threats to our systems.

Having put in context how the bill will help our mission and improve the security of Federal systems, let me state our clear desire to work with the Committee and the bill's sponsors to improve the bill's provisions based on the following observations and suggestions. In making these points, I want to divide our comments between the provisions that were drawn from the original Computer Security Enhancement Act, and those that have been incorporated from H.R. 1572, introduced earlier this year. As I just indicated, a number of provisions in this bill are carried over from earlier versions of the Computer Security Enhancement Act. Let me address those.

First, the bill proposes in Section 4 to assign NIST responsibility "to coordinate Federal response efforts related to unauthorized access to Federal computer systems." NIST can certainly play an important role in developing guidance on responding to incidents, including unauthorized intrusions. We do not believe it is appropriate to place NIST in a central operational capacity to coordinate specific agency responses to specific intrusions. Rather, agencies need to have programs and procedures in place, drawing upon NIST guidance, to address such situations, including appropriate coordination with law enforcement personnel.

Second, Section 5 would require NIST to emphasize the development of technology-neutral policy guidelines for computer security practices by Federal agencies. Technology neutrality is consistent with the Government Paperwork Elimination Act, with respect to the legal effect of authentication technologies. That said, specific technologies have differing security strengths, costs, and benefits. They are not interchangeable from a security point of view. We take this into account in our choices of technical work activities. While policy guidelines should be neutral, Federal agencies need to know the benefits and costs of various technologies to facilitate the selection of appropriate security solutions to meet specific agency missions and customer needs. We do not want this section to be misinterpreted to preclude appropriate technical activities and the development and issuance of needed specific technical guidance and standards.
Third, Section 6, as currently written would require NIST to solicit recommendations of the Computer System Security and Privacy Advisory Board before submitting a proposed Federal standard to the Secretary, and to submit the Board's recommendation along with the proposed standard to the Secretary. We currently inform the Board of proposed standards during our public comment process, solicit their comments and welcome their recommendations and views. Of course, we cannot compel the Board to make a recommendation on any particular matter. As currently drafted, this provision could delay the approval of a needed standard. For example, from time to time, a serious flaw may be found in a standard, requiring immediate corrective action, and sometimes we issue non-controversial standards that raise no significant technical or policy issues. We agree with the intent of this section, however, and we would be happy to work with the Committee to develop language that would enable NIST and the Board to continue to work together in a timely and productive fashion.

Fourth, Section 7, "Limitation on Participating in Requiring Encryption Standards" would prohibit NIST from promulgating, enforcing, or otherwise adopting standards for the Federal establishment of encryption standards required for use in computer systems other than Federal Government computer systems. Although NIST does not have any authority -- and no desire -- to impose encryption standards on the private sector, we are concerned that this language might be misunderstood to preclude NIST from collaborating with the private sector on standards that are likely to be used by both the private and public sector. For instance, NIST works closely with the American National Standards Institute's (ANSI) banking standards community on voluntary security for use by the financial services industry. We would not want such productive work to be precluded. Again, we would be happy to work with the Committee to develop clearer language.

Let me now turn to provisions that appear to be drawn from H.R. 1572, introduced earlier this year.

As this Committee knows, the Administration has articulated a workable policy in this area that promotes market-driven, industry approaches to the issue of authentication. In many respects, the private sector is moving to examine the issues related to authentication and implement appropriate technologies and models to meet real needs. Likewise, our government agencies -- at both Federal and state levels -- are developing the experience and testing models for how best to provide authentication mechanisms that work, provide confidence, and meet specific needs of both users and agencies.

The Administration is committed to using the new information technologies to enable electronic transactions between government agencies and their customers. That is why we supported the

Government Paperwork Elimination Act, which the President signed into law last year. As directed by that statute, the Office of Management and Budget has issued draft implementing guidance on electronic signatures, and is now in the process of formulating final guidance -- based on public comments -- to meet that law's April 2000 deadline.

Section 13(a)-(d) call for NIST, to develop guidelines specifying how agencies would implement various authentication methods, minimum interoperability specifications, and validation criteria for testing, as well as minimum technical criteria for the use of electronic certification and management systems. We would like to work with the Committee to address a number of implications of these provisions.

To the extent that more detailed guidelines, criteria, and evaluations are desirable, it would be appropriate to tie them to the guidance required by existing law. Thus, following issuance of the final guidance, it might be appropriate for the Director of NIST to convene government and industry representatives to discuss the merits of developing more detailed guidance that, for example, linked the OMB criteria more clearly to the specific characteristics of products available in the commercial marketplace. That might enable government agencies to make more informed purchasing decisions.

Turning to Section 11, we believe that the NRC study described in that provision would develop useful information concerning the use of public key infrastructures by individuals, business, and government. That would supply a valuable baseline for future action in this area.

Finally, Section 13(e) establishes a "National Policy Panel for Digital Signatures" in the Office of the Under Secretary. We would like to work with the Committee on this proposal, keeping in mind Administration policy that standards and practices in the area of electronic commerce should be industry and market driven. The Panel would be empowered to develop model practices and procedures, guidelines and standards, and audit procedures. We have concerns that this could be interpreted as the Government writing and publishing standards for the private sector. We would like to work with private sector organizations already involved in this effort and who are focusing the product of their effort on specific industry needs. The NRC study could provide important input for this determination.

Thank you again for the opportunity to testify today on the Computer Security Enhancement Act of 1999. We look forward to working with the Committee and accomplishing our mutual goal of strengthening the security of Federal systems. At this time I would be happy to answer any questions that the Committee might have.

NIST Office of the Director

Mr. Raymond Kammer, Director

Raymond Kammer was nominated by President Clinton on September 4, 1997, to serve as Director of the National Institute of Standards and Technology. After being confirmed by the U.S. Senate, he took office on November 12. An agency of the U.S. Commerce Department's Technology Administration, NIST promotes U.S. economic growth by working with industry to develop and apply technology, measurements, and standards. As NIST Director, Mr. Kammer oversees a staff of approximately 3,300 and a budget of about $700 million. More than half of the staff is composed of scientists and engineers located at the NIST campuses in Gaithersburg, Maryland, and Boulder, Colorado.

Most recently, Mr. Kammer served on an acting basis as the Chief Financial Officer, the Assistant Secretary for Administration and the Chief Information Officer for the Department of Commerce. As Deputy Director of NIST from 1980 to 1991 and 1993 to 1997, Mr. Kammer was responsible for the day-to-day operation of the Institute and for long-range planning and policy development. The primary mission of NIST is to strengthen the U.S. economy and improve the quality of life by working with industry to develop and apply technology, measurements, and standards. It carries out this mission through a portfolio of four major programs:

- Measurement and Standards Laboratories that provide technical leadership for vital components of the nation's technology infrastructure needed by U.S. industry to continually improve its products and services;

- the Advanced Technology Program, accelerating the development of innovative technologies for broad national benefit through R&D partnerships with the private sector;

- a grassroots Manufacturing Extension Partnership with a network of local centers offering technical and business assistance to smaller manufacturers; and

- a highly visible quality outreach program associated with the Malcolm Baldrige National Quality Award that recognizes business performance excellence and quality achievement by U.S. manufacturers, service companies, educational organizations, and health care providers.

From 1991 to 1993, Mr. Kammer was Deputy Under Secretary of Commerce for Oceans and Atmosphere in NOAA. In that position, he served as NOAA's Chief Operating Officer and was responsible for overseeing the technical projects of this $2 billion agency which has a staff of over 14,000. NOAA has five major programs - the National Weather Service; the National Marine Fisheries Service; the National Environmental Satellite, Data, and Information Service; the National Ocean Service; and the Office of Oceanic and Atmospheric Research.

Mr. Kammer began his career with the Department of Commerce in 1969 as a program analyst. Prior to his appointment as Deputy Director of NIST, Mr. Kammer held a number of positions at NIST and in the Department of Commerce involving budgetary and program analysis, planning and personnel management. During his tenure as Deputy Director, he also held positions as Acting Director of NIST, Acting Director of the National Measurement Laboratory at NIST, and Acting Director of the Advanced Technology Program at NIST.

Mr. Kammer has chaired several important evaluation committees for the Department of Commerce, including reviews of satellite systems for weather monitoring and the U.S. LANDSAT program, and of the next generation of weather radar used by the U.S. government. He also served on the Board of Directors of the American Society for Testing and Materials, a major international society for the development of voluntary standards for materials, products, systems, and services.

His awards include both the Gold and Silver Medals of the Department of Commerce, the William A. Jump Award for Exceptional Achievement in Public Administration, the Federal Government Meritorious Executive Award, and the Roger W. Jones Award for Executive Leadership.

..r. Kammer received his Bachelor of Arts degree from the University of Maryland in 1969.

Chairwoman MORELLA. I was just discussing your—the contest you have for designing a DES replacement. Thank you. Thank you, Mr. Kammer.

Now a pleasure to hear from Mr. Rhodes.

STATEMENT OF KEITH RHODES

Mr. RHODES. Madam Chairwoman, members of the Subcommittee, thank you for asking me to participate in today's hearing on the proposed Computer Security Enhancement Act of 1999.

Today, I would like to discuss, one, the urgent need to strengthen computer security across the Federal Government; two, the current and future privacy concerns with any computer security legislation; three, our views on the proposed act, and, four, what can be done to further strengthen security program management at individual agencies as well as Government-wide leadership coordination and oversight.

Over the past year, this Subcommittee has held a series of hearings focused on security issues, such as the break-ins of federal webs sites and the Melissa computer virus. While these incidents resulted in relatively limited damage, they demonstrated the formidable challenge that the Federal Government faces in protecting its information systems assets and sensitive data.

It is imperative, therefore, that the Federal Government swiftly implement long-term solutions both at individual agencies and Government-wide to protect systems and sensitive data. These include strengthening security management by individual agencies; clarifying the roles of various federal organizations with responsibilities related to information security; identifying and ranking the most significant information security issues facing federal agencies; ensuring the adequacy of information technology workforce skills; periodically evaluating and testing agency information security practices, and assuring high level executive branch leadership.

Regarding privacy issues, this Subcommittee is well aware that developing and implementing information security legislation can be a delicate balancing act. The need to protect sensitive data and systems must be weighed not only against cost and feasibility concerns but also the privacy and security interests of individual citizens, private businesses, as well as national security and law enforcement agencies. However, without computer security, privacy cannot be assured.

For individuals in the private sector, the Internet is rapidly becoming a popular business avenue. Not surprisingly, security and privacy concerns have increased along with the popularity of this electronic commerce. Customers are primarily concerned with credit card fraud which has increased considerably over the past several years, but concerns are also growing about identifying theft as well.

Businesses are interested in protecting customers as well as their own information assets from competitors, vandals, criminals, suppliers, and foreign governments. An important part of the solution to these security concerns is cryptography. While information vulnerabilities cannot be eliminated through the use of any single tool, cryptography can help businesses ensure the confidentiality and integrity of information and verify the asserted identity of individuals and computer systems. However, national security and law enforcement concerns must be considered as cryptographic tools become increasingly available. Thus, without obtaining agreement among individual users, businesses, law enforcement, national security, and other authorities on the requirements, there is no way to build and implement the new technology or to establish standards that will be universally accepted.

The proposed Computer Security Act of 1999 takes a number of steps to address the proliferation of network systems and the corresponding need for better protection over sensitive data belonging to both Government and the private sector. If effectively implemented, these provisions can have a positive impact in addressing information security problems identified in our audits.

The bill particularly focuses on the role NIST plays in assisting federal agencies to protect their systems and promote technology solutions to security protection based on private sector offerings. While this legislation provides an improved basis for protecting critical federal assets, it is important to recognize that there is no legislative substitute that could be put in place to provide the increased management attention and due diligence necessary to implement and ensure the effectiveness of information security controls.

It is also important to ensure that NIST retain its role as an honest broker in the development of security standards for unclassified data which industry standards—and deciding which industry standards are appropriate for federal agencies, that NIST have the capability and authority to execute its mission, and that agencies themselves consistently implement such standards.

As stated earlier, it is important to recognize that in the long-term a more comprehensive, government-wide strategy needs to emerge to ensure that critical federal assets and operations are protected from evolving security threats. This strategy needs to address two of the most fundamental deficiencies in federal computer security: one, poor agency security program planning and management, and, two, ineffective government-wide oversight.

Madam Chairwoman, this concludes my testimony. I will be happy to answer any questions you or any of the members of the Subcommittee have.

[The statement of Mr. Rhodes follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology, Committee on Science, House of Representatives

For Release on Delivery
Expected at 1:30 p.m.
Thursday
September 30, 1999

INFORMATION SECURITY

The Proposed Computer Security Enhancement Act of 1999

Statement of Keith A. Rhodes
Director, Office of Computer and Information Technology Assessment
Accounting and Information Management Division

GAO
Accountability * Integrity * Reliability

GAO/T-AIMD-99-302

Madam Chairwoman and Members of the Subcommittee:

Thank you for asking me to participate in today's hearing on the proposed Computer Security Enhancement Act of 1999 (H.R. 2413). The legislation seeks to address the dramatic advances in information technology that have occurred since the Computer Security Act of 1987[1]--advances which have significantly increased risks to our computer systems and, more importantly, to the critical operations and infrastructures they support. In particular, H.R. 2413 aims to reinforce the role of the National Institute of Standards and Technology (NIST), whose mission is to provide guidance and technical assistance to government and industry to protect unclassified information systems.

Today, I would like to discuss (1) the urgent need to strengthen computer security across the federal government, (2) the current and future privacy concerns with any computer security legislation, (3) our views on the proposed act, and (4) what can be done to further strengthen security program management at individual agencies as well as governmentwide leadership, coordination and oversight.

[1] The primary objectives of this act were to provide for (1) a computer standards program within NIST, (2) security and privacy for information in federal computer systems not covered by national security restrictions and (3) training in security matters for persons involved in the management, operation, and use of federal computer systems.

THE URGENT NEED TO STRENGTHEN COMPUTER SECURITY FOR THE FEDERAL GOVERNMENT

As hearings by this Subcommittee have recently emphasized, risks to the security of our government's computer systems are significant, and they are growing. The dramatic increase of computer interconnectivity and the popularity of the Internet, while facilitating access to information, are factors that also make it easier for individuals and groups with malicious intentions to intrude into inadequately protected systems and use such access to obtain sensitive information, commit fraud, or disrupt operations. Further, the number of individuals with computer skills is increasing, and intrusion, or "hacking," techniques are readily available.

Attacks on and misuse of federal computer and telecommunications resources are of increasing concern because these resources are virtually indispensable for carrying out critical operations and protecting sensitive data and assets. For example, system break-ins at the Department of the Treasury could place billions of dollars of annual federal receipts and payments at risk of fraud and large amounts of sensitive taxpayer data at risk of inappropriate disclosure. At the Department of Defense, operations such as mobilizing reservists, paying soldiers, and managing supplies could be affected as well as warfighting capability. At the Health Care Financing Administration, billions of dollars of claim payments and sensitive medical information could be affected.

Over the past year, this Subcommittee has focused[2] on a series of break-ins of federal web sites and the "Melissa" computer virus.[3] While these incidents resulted in relatively limited damage, they demonstrated the formidable challenge that the federal government faces in protecting its information systems assets and sensitive data. For example, Melissa and other recent viruses, such as "Explore Zip",[4] showed just how quickly attacks can proliferate due to the intricate and extensive connectivity of today's networks—in just days after the virus was unleashed, there were widespread reports of "infections" throughout the country. They also demonstrated that vulnerabilities in commercial-off-the-shelf (COTS) products, which federal agencies are increasingly relying on to support critical federal operations, can be easily exploited to attack all their users.

Because of the increasing reliance on the Internet and standard COTS products, as well as the increasing improvements in computer attack tools and techniques

[2] Information Security: The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data (GAO/T-AIMD-99-146, April 15, 1999); Information Security: Recent Attacks on Federal Web Sites Underscore Need for Stronger Information Security Management (GAO/T-AIMD-99-223, June 24, 1999); Information Security: Answers to Posthearing Questions (GAO/AIMD-99-272R, August 9, 1999).

[3] Melissa was a "macro virus" that could affect users of Microsoft's Word 97 or Word 2000 word processing software. Macro viruses are computer viruses that use an application's own macro programming language to reproduce themselves. The viruses can inflict damage to the document or to other computer software.

[4] ExploreZip was a virus designed to destroy electronic files, degrade network performance, and eventually cause a denial of service on electronic mail servers.

(as evidenced in the additional capability and techniques deployed in the recent virus attacks), it is likely that the next virus will propagate faster, do more damage, and be more difficult to detect and counter. Yet audits reports issued by us and agency inspectors general since 1996 have found that many agencies are not prepared to protect themselves from these evolving threats.

It is imperative, therefore, that the federal government swifty implement long-term solutions both at individual agencies and governmentwide to protect systems and sensitive data. As I will further discuss today, these include: strengthening security management by individual agencies; clarifying the roles of various federal organizations with responsibilities related to information security; identifying and ranking the most significant information security issues facing federal agencies; ensuring the adequacy of information technology workforce skills; periodically evaluating and testing agency information security practices; and assuring high-level executive branch leadership.

In recent years, NIST has had a valuable role in helping agencies to protect unclassified information systems and addressing advances in security technology. Since enactment of the Computer Security Act of 1987, NIST has had the responsibility for setting computer security standards for all federal agency systems except national security systems. National security system standards are set by the National Security Agency. NIST has also undertaken efforts to raise awareness of information technology vulnerabilities and protection requirements; facilitate the development of new technologies to provide system and network protection; and develop guidance to ensure effective security planning and management.

COMPUTER SECURITY LEGISLATION AND PRIVACY CONCERNS

Developing and implementing information security legislation can be a delicate balancing act. The need to protect sensitive data and systems must be weighed not only against cost and feasibility concerns but also the pnvacy and security interests of individual citizens, private businesses, as well as national security and law enforcement agencies. However, without computer security, privacy cannot be assured.

For individuals and the private sector, the Internet is rapidly becoming an increasingly popular avenue of doing business. A study jointly sponsored by the University of Texas Center for Research in Electronic Commerce and Cisco Systems, Inc.[5] found that the Internet economy generated more than $300 billion in U.S. revenue and was responsible for 1.2 million jobs in 1998. The study also found that Internet commerce is growing at a much faster rate than expected—in 1998, total electronic commerce exceeded $102 billion for U.S.-based companies. Not surprisingly, security and privacy concerns have increased

[5] See www.internetindicators.com for details on this study's findings.

along with the popularity of electronic commerce. Customers are primarily concerned with credit card fraud, which has increased considerably over the past several years. Businesses are interested in protecting customers as well as their own information assets from competitors, vandals, criminals, suppliers, and foreign governments.

An important part of the solution to these security concerns is cryptography. Information that has been properly authenticated and encrypted cannot be understood or interpreted by those lacking the appropriate cryptographic key. While information vulnerabilities cannot be eliminated through the use of any single tool, cryptography can help businesses ensure the confidentiality and integrity of information in transit and storage and verify the asserted identity of individuals and computer systems.

However, national security and law enforcement concerns must be considered as cryptographic tools become increasingly available. For example, encryption can prevent law enforcement authorities from gaining access to information needed to investigate and prosecute criminal activity. It can also threaten intelligence gathering for national security purposes.

At the same time, the use of encryption by the private sector can benefit law enforcement and national security interests. According to the National Research Council, by protecting the trade secrets and proprietary information of businesses, encryption can reduce economic espionage, and thus support the job of law enforcement. By helping protect nationally critical information systems and networks (e.g., banking, telecommunications, and electric power) against unauthorized penetration, encryption can support the national security of the United States.[6]

Not only does this complex web of interests make it difficult to draft effective security legislation, it also makes it challenging to develop cryptographic and other security technology. Without obtaining agreement among individual users, businesses, law enforcement, national security and other authorities on requirements, there is no way to build and implement the new technology or to establish standards that will be universally accepted.

THE COMPUTER SECURITY ENHANCEMENT ACT TAKES POSITIVE STEPS TOWARD ADDRESSING DRAMATIC ADVANCES IN INFORMATION TECHNOLOGY

The proposed Computer Security Enhancement Act of 1999 takes a number of steps to address the proliferation of networked systems and the corresponding need for better protection over sensitive data belonging to both government and the private sector. If effectively implemented, these provisions can have a

[6] Cryptography's Role in Securing the Information Society, National Research Council, May 1996.

positive impact in addressing information security problems identified in our audits.

The bill particularly focuses on the role NIST plays in assisting federal agencies to protect their systems and promote technology solutions to security protection based on private sector offerings. While this legislation provides an improved basis for protecting critical federal assets, it is important to recognize that there is no legislative substitute that could be put in place to provide the increased management attention and due diligence necessary to implement and ensure the effectiveness of information security controls. It is also important to ensure that NIST retain the ability to develop security standards for unclassified data and decide which industry standards are appropriate for federal agencies, and that agencies themselves consistently implement such standards.

I would now like to comment on a few provisions in the bill that focus on NIST's role in helping agencies to protect their systems and ensure that NIST will play a vital role in helping to pioneer new security technologies.

First, the bill requires NIST to provide guidance and assistance to federal agencies in the protection of interconnected systems and to coordinate federal response efforts related to unauthorized access to federal computer systems. We support this measure as federal response efforts have been sporadic and uneven to date. However, it will be important to make sure that NIST has the capability and authority needed to carry out this function.

Second, the bill requires the Under Secretary of Commerce to establish a clearinghouse of information available to the public on information security threats. We support the establishment of a clearinghouse; however, to be effective, it will be important for the information provided by the clearinghouse to be complete and useful for analyses of widespread attacks. As you may recall, when the Melissa virus surfaced earlier this year, we found that there was no single place to obtain complete data on which agencies were hit and how they were affected. Moreover, there was no data available that quantified the impact of the virus in terms of productivity lost or the value of data lost. Also, it may be necessary to clarify requirements for reporting incidents. Because there are several entities already providing information on information security threats--including the FBI and the FedCIRC[7]-- it may be unclear to many agencies where incidents should be reported. Finally, it is important to recognize that, by itself, a clearinghouse is not a panacea to information security problems across the federal govemment. Agencies themselves must still use this information effectively to assess risks to their own computer-supported operations and to develop and implement sound management controls.

[7] FedCIRC—the Federal Computer Incident Response Capability—is a reporting center at the General Services Administration.

Third, the bill requires the National Research Council to conduct a study to assess the desirability of public key infrastructures (PKIs) and the technologies required for the establishment of such key infrastructures. Public key cryptography uses two electronic keys: a public key and a private key. A public key infrastructure provides the means to bind keys to their owners and helps in the distribution of reliable public keys in large networks.[8] As the use of the Internet by federal agencies, businesses and citizens continues to expand, it is important that the benefits as well as the vulnerabilities of PKI as well as implementation concerns be thoroughly examined. For instance, the widespread use of PKI technology can help increase the confidence of electronic transactions, but to be effective, PKI components need to interoperate regardless of the source of the equipment and software involved and they also need to be adequately secured. NIST has already been working with industry and technical groups to advance PKI technology and to develop standards that provide a basis for interoperable components, and we support these efforts.

Fourth, the bill establishes a National Policy Panel for Digital Signatures for the purpose of exploring issues relevant to the development of a national digital signature infrastructure based on uniform standards and of developing model practices and standards associated with certification authorities. Again, with the

[8] According to NIST, public and private keys are mathematically related but the private key cannot be determined from the public key. The public key can be known by anyone while the private key is kept secret by its owner. As long as there is a strong binding between the owner and the owner's public key, the identity of the originator of a message can be traced to the owner of the private key. Public keys may be bound to their owners by public key certificates. These certificates contain information such as the owner's name and the associate public key and are issued by a reliable certification authority.

explosive growth of the Internet, there is an increasing demand for confidentiality and integrity with electronic commerce transactions. This means that the receiver of an electronic commerce message must be assured that the message came from the actual sender, that no part of the message has been altered during transmission, and that the contents of the transaction have been kept confidential. NIST has already been working with industry to test digital signature technology and to develop new approaches. We also support these efforts as they will ensure that NIST is well-positioned to assist in electronic commerce standardization efforts.

THE NEED FOR A BROADER INFORMATION SECURITY IMPROVEMENT FRAMEWORK

As stated earlier, it is important to recognize that, in the long term, a more comprehensive governmentwide strategy needs to emerge to ensure that critical federal assets and operations are protected from evolving security threats. This strategy needs to address two of the most fundamental deficiencies in federal computer security: (1) poor agency security program planning and management and (2) ineffective governmentwide oversight.

At the agency level, a number of factors have consistently contributed to poor federal information security, including insufficient awareness and understanding of risks; a shortage of staff with needed technical expertise; a lack of systems and security architectures to facilitate implementation and management of securnty controls; and various problems associated with the availability and use of specific technical controls and monitoring tools. A more important underlying problem, however, is a lack of security program management and oversight to ensure that risks are identified and addressed and that controls are working as intended.

In our September 1998 report[9] on the overall state of federal information security, we noted that of 17 agencies where security planning was reviewed, all had deficiencies. Many agencies had not developed security plans for major systems based on risk, had not formally documented security policies, and had not implemented a program for testing and evaluating the effectiveness of the controls they relied on.

Recently, for example, we reported[10] that penetration tests we conducted at one of the National Aeronautics and Space Administration's (NASA) 10 field centers showed that mission-critical systems responsible for command and control of spacecraft as well as the processing and distributing of scientific data retumed from space were vulnerable to unauthorized access. A major contributing factor to our ability to penetrate these systems was that NASA was not effectively and

[9] Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92, September 1998).

[10] Information Security: Many NASA Mission-Critical Systems Face Serious Risks (GAO/AIMD-99-47, May 20, 1999).

consistently managing IT security throughout the agency. Specifically, it was not effectively assessing risks to its systems; implementing security policies and controls; monitoring policy compliance or the effectiveness of controls; providing required computer security training; and centrally coordinating responses to security incidents. In commenting on our report, NASA concurred with our findings and is taking actions to implement our recommendations.

To help agencies implement the kind of management framework that is required to effectively respond to evolving security requirements, we issued an executive guide in May 1998 entitled Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68). It describes a framework for managing risks through an ongoing cycle of activities coordinated by a central focal point. The guide, which is based on the best practices of organizations noted for superior information security programs, has been endorsed by the Chief Information Officers (CIO) Council. By adopting the practices recommended by the guide, agencies can be better prepared to protect their systems, detect attacks, and react to security breaches.

With regard to governmentwide oversight, over the last several years, a number of efforts have been initiated to strengthen central oversight and coordination for information security. For example, the Security Committee established by the CIO Council has taken steps to promote security awareness, improve agency access to incident response services, and support agency improvement efforts.

Also, Presidential Decision Directive (PDD) 63, issued in May 1998, called for a range of actions intended to improve federal agency computer security programs, establish a partnership between the government and private sector, and improve our nation's ability to detect and respond to serious attacks. It created several new entities for developing and implementing a strategy for critical infrastructure protection and it tasked federal agencies with developing critical infrastructure protection plans. Since then a variety of activities have taken place, including development and review of individual agency protection plans, identification and evaluation of information security standards and best practices, and efforts to build communication links with the private sector.

However, a number of issues still need to be resolved. At present, for example, there is no mechanism, such as required independent audits, for routinely testing and evaluating the effectiveness of agency information security programs.[11] As a result, little useful information is routinely available for measuring the effectiveness of agency security programs, and thus, holding agency managers accountable and identifying and addressing the most serious problems. Also, the proliferation of organizations with overlapping oversight and assistance responsibilities is a source of potential confusion among agency personnel and may be an inefficient use of scarce technical resources. Exacerbating this problem is confusion over which information security standards and guidance are mandatory, rather than optional.

[11] Some independent testing of systems is done through agency annual financial statement audits.

Thus, as we previously recommended in 1998,[12] to substantively improve protection over sensitive data and critical infrastructures, the Congress needs to consider stronger measures that would ensure that executive agencies are doing the following.

- Carrying out their responsibilities outlined in laws and regulations requiring them to protect their information resources.
- Clearly delineating the roles of the various federal organizations with responsibilities related to security.
- Identifying and ranking the most significant information security issues facing federal agencies.
- Promoting information security risk awareness among senior agency officials whose critical operations rely on automated systems.
- Strengthening information technology workforce skills.
- Evaluating the security of systems on a regular basis.
- Providing for periodically evaluating agency performance from a governmentwide perspective and acting to address shortfalls.

[12] GAO/AIMD-98-92.

Madam Chairwoman, this concludes my testimony. I will be happy to answer any questions you or Members of the Subcommittee may have.

(511862)

Keith A. Rhodes

BIOGRAPHICAL SKETCH

Mr. Rhodes has been the Director of AIMD's Office of Computer and Information Technology Assessment since May 1999, providing assistance throughout GAO on computer and telecommunications technology issues, and participating in reviews requiring significant technical expertise. Prior to assuming his current position, he served as Technical Director in the Chief Scientist's Office, providing technical analysis on a range of GAO assignments such as the Year 2000 computer crisis, computer and information security, system modernization efforts at the IRS, FAA, and NWS. as well as various weapon systems. Immediately before joining GAO in 1991, he was a supervisory computer specialist at the Lawrence Livermore National Laboratory. His other work experience includes computer and telecommunications projects at Northrop Corporation and Ohio State University.

Mr. Rhodes holds graduate degrees in computer engineering and engineering physics from the Ohio State University and the University of California (Los Angeles), respectively. Throughout his career, he has garnered numerous awards and citations, including the 1999 Arthur S. Flemming Award for Applied Science. He is a Professional Engineer, a Certified Computing Professional, and a member of the New York Academy of Science. He holds two patents in automated control systems and has authored numerous articles on computer security, performance modeling of communication networks and computer architecture for several technical journals.

Chairwoman MORELLA. Thank you, Mr. Rhodes.

I note that Ms. Stabenow has joined our panel here on the Subcommittee.

I'd like to now recognize Mr. Harris Miller.

STATEMENT OF HARRIS MILLER

Mr. MILLER. Thank you, Chairwoman Morella and members of the Subcommittee. I want to apologize to the Subcommittee for getting my testimony to you late, but I've been in Buenos Aires most of last week talking about information security, actually, at a major global conference, so it's very appropriate.

I also want to thank the Chair for mentioning my selection by the Washingtonian as an influential executive. A lot of that's due to the fact that this Subcommittee has been a leader on Y2K, because I think a lot of my recognition is a recognition of the work our Association has done on the Y2K issue, and if we're considered again for such an award, I think it would be because of our information security work. So, I really commend you again for focusing on this issue.

In general, Madam Chair, we strongly endorse this bill and believe it's very appropriate. And I'd just like to make about three quick points here before the Subcommittee today.

Number one, as important as the role of NIST was in 1987 in terms of playing an important role within the federal civilian agencies in information security, it is much more important in 1999, because the whole issue of information security in the civilian agencies has become much more important.

The Internet, the growth of Internet technology, the growth of network systems, the vulnerability of those systems simply makes it much more important that there be the kind of expertise and focus that you have at NIST to help the federal agencies on the civilian side. On the defense side, on the national security side, it's a different set of issues. But NIST needs to be strengthened, and the overall thrust of this legislation in that direction to provide more leadership, more resources to NIST is something that the Congress should quickly move to endorse, and that alone is a reason to endorse this legislation.

I think a second general point which I see very clearly enunciated in this legislation, which the members of the Information Technology Association of America support, is continued industry leadership, and I refer to the point that Mr. Gordon made in his opening remarks and Mr. Kammer made in his remarks, that clearly industry leadership here is critical, and working with NIST in a collaborative way is the way to go rather than looking at the idea that somehow standards means NIST or anybody else in the Government directing the industry in which way to go.

And I refer the Subcommittee in some detail in my written comments to, for example, the Federal Electronic Commerce Coalition, which ITAA is working with many other high-tech trade associations and the Department of Defense initially, and we expect to also work with civilian agencies to help develop best practices and develop the idea of collaboration between industry and Government and within the Government itself. And, again, it's not a standard-setting body; it's sharing information.

And we're already off to a very positive start. Deputy Secretary of Defense, Dr. Hamre is very much behind this, and we expect this to be a model of how to share information, and certainly in the area of information security the same idea should obtain, that there can be a collaborative, cooperative effort between industry and Government but not top-down dictated standards, and I appreciated Mr. Gordon's comments about rewording the particular sections of his provisions of the bill.

Thirdly, I think that there continue to be great opportunities for collaboration between industry and Government in the information security area. Just this past week, we announced with the Department of Justice a grant from the Department of Justice to ITAA where we will be working with DOJ on a cybercitizen education project where we'll be developing materials designed to reach out as an initial population to younger people to educate them about information security and the need to be good cybercitizens.

And you may say, "Well, what does this have to do with the topic today?" Well, it has two things to do with the topic today. Number one is, as the bill correctly points out, we need more resources to train specialists in information security. I recently talked to one of my member companies, which does a lot of work for the United States Government information security. The senior manager told me he has need for 1,500 people; he has 1,000 available. He's already short 500 people. And because these are for Government agencies, this is not the kind of problem we can solve through H1–Bs.

And, as the Chairwoman knows, I support the H1-B Program, but you can't support this by bringing in immigrants. You can't solve this problem by outsourcing it to another country. We need to have specialists trained in this country. So, the bill's thrust, to train more information security specialists, is very positive.

The second reason the cybercitizen project is important is that it helps to build up the idea that we need to work together to deal with cyber protection. This is not just an issue for industry and not just an issue for Government.

And the fourth issue that I wanted to address in general is the fact that there are additional resources needed. When I testified before the Subcommittee in another hearing recently, we discussed the fact that the Commerce Department NTIA Program was being defunded for information security in that area, which is unfortunate, and I don't think any money was put back in even though I know the Chairwoman and Congressman Horn were both concerned about that, as was Ms. Rivers at that last hearing.

Now, we have a request from the Administration, as Mr. Kammer pointed out, for additional money. I hope that the Congress will see fit to put that money in. In the grand scheme of things, it's not a lot of money. I know the budget's tight and the budget caps are tight. But, again, like Y2K, it's like that old Fram air filter commercial, "You can pay me today or you can pay me later." I think that spending this money now by the Congress to promote information security in the Federal Government, in the civilian agencies, as well as in the Defense and National Security agencies, will save the country and will save the Government a lot of funds over the long term.

So, in sum, again, we endorse the bill. We have in our detailed written testimony some minor suggested changes but generally we think it's a very positive step and urge positive Congressional action on the legislation.

[The statement of Mr. Miller follows:]

"The Computer Security Enhancement Act of 1999: H.R. 2413"

Testimony of

Harris N. Miller,
President
Information Technology Association of America

Presented to:

House Committee on Science
Subcommittee on Technology

September 30, 1999

Introduction

I am Harris Miller, President of the Information Technology Association of America (ITAA), representing over 11,000 direct and affiliate member companies in the information technology (IT) industry - the enablers of the information economy. Our members are located in every state in the United States, and range from the smallest IT start-ups to industry leaders in the custom software, services, systems integration, telecommunications, Internet, and computer consulting fields. These firms are listed on the ITAA website at www.itaa.org.

Chairwoman Morella, Subcommittee Members, I want to commend you and your colleagues for holding this hearing on H.R. 2413, the Computer Security Enhancement Act of 1999 (CSEA). It is an honor to appear before your Subcommittee, which has been instrumental in moving government and industry forward on addressing a related critical IT issue: the Y2K computer problem. As a result of your Subcommittee's leadership, we as a nation are much further along in fixing the Y2K problem than many would have ever expected even one year ago.

I. InfoSec: Economic Impact on US

In light of your Y2K leadership, it is particularly appropriate for your Subcommittee to be holding this hearing and reviewing this legislation. As I testified before a joint hearing of this Subcommittee and Chairman Horn's Subcommittee on Government Management, Information, and Technology on August 4, 1999, ITAA strongly believes that Information Security (InfoSec) will be the next Y2K issue for the information technology (IT) industry. What I mean by that statement simply is that InfoSec will require the attention of government and industry around the globe to prevent major threats to our global economy and society.

First, frequent reports of vulnerabilities of IT systems are one indicator of the significance of InfoSec. One lesson we all may have learned from the Year 2000 challenge is that information technologies now are pervasive, complex and critical—operating the essential functions of business and government. As recent headlines indicate, a number of government and industry computer systems have been under "cyber attack." We have seen attacks on government in many forms—whether the targets were national defense systems or Congressional Web pages. American businesses also are experiencing the effects of cyber attacks—from teenagers engaging in pranks to experts attempting corporate espionage.

As the development and adoption of Electronic Commerce (EC) remains in a nascent stage, the issue of "trust" becomes increasingly important. Businesses, government and citizens alike must trust the security of their information and the identity of the person or company on the other end. They must know the systems they are using are reliable. Events that shake this trust—whether real or perceived—pose a threat to the development of EC and the continued outstanding growth of the IT industry.

But this is not simply an issue of growth for our industry; rather, as a number of reports indicate, IT growth is fueling the growth of the US and global economy. Information technology represents over 6 percent of global gross domestic product (GDP), a spending volume of more than $1.8 trillion, and over 8% of US GDP, according to Digital Planet, a report recently released by the World Information Technology and Services Alliance (WITSA). WITSA is a group of 39 IT trade associations around the world, and I am proud to serve as President. Enormous in its own right, the Digital Planet figures mask the contribution made by this technology to the growth, competitiveness and vitality of other industries. From China to Mexico, from Argentina to Germany, countries have come to recognize that IT is the engine of national development, accelerating the expansion of business opportunity and investment while acting as a buffer against economic downtums. The recent US Department of Commerce report indicates that an incredible 35% of the nation's real economic growth from 1995 to 1998 came from IT.

Because of these connections between EC, the IT industry, and the global economy, any threat to the reliability of information systems poses potential threats to the delivery of services to the American public and to the economic health of our nation, and other nations around the world. The WITSA Global Public Policy Summit from which I just retumed in Buenos Aires, Argentina, had global InfoSec challenges as a major agenda item.

Industry already has begun to address the InfoSec issue through industry-led actions. In our role as Sector Coordinator for the Information and Communications sector, appointed by the U.S. Department of Commerce, ITAA and its member companies are raising awareness of the issue within the IT industry and through partnership relationships with other vertical industries, including finance, telecommunications, energy, transportation, and health services. We are developing regional events, conferences, seminars and surveys to educate all of these industries on the importance of addressing information security. Through our ITAA InfoSec committee, our member companies also are exploring joint research and development activities, international issues, and security workforce needs.

In addition to our industry-led efforts, ITAA is working in collaboration with the Federal govemment. ITAA recently formed a "Cybercitizen Partnership" with the U.S. Department of Justice to begin developing an educational program in an effort to reduce the potential of children to engage in cybercrime. We also continue to collaborate with the Critical Infrastructure Assurance Office (CIAO) and the interagency Education and Awareness Committee on building a Govemment/Industry partnership to address InfoSec.

II. ITAA Support: Broad Themes of HR 2413

First, allow me to begin by expressing ITAA's support of a number of stated goals and broad themes conveyed by H.R. 2413.

Stated Goals

According to Science Committee Chairman James Sensenbrenner's remarks introducing H.R, 2413, CSEA is intended to accomplish two goals: (1) assist the National Institute of Standards and Technology (NIST) "in meeting the ever-increasing computer security needs of Federal civilian agencies," and (2) to "allow the Federal Government, through NIST, to harness the ingenuity of the private sector to help address its computer security needs."

ITAA supports both goals, both in what they specify and what they imply. First, for the reasons I mentioned above, ITAA acknowledges that the need for computer security for Federal civilian agencies is increasing—similar to what is being faced by businesses and other governments around the globe. We support Federal efforts that result in increased actions by the civilian agencies to address computer security.

Secondly, ITAA strongly supports the second goal, particularly its stated reference to the "ingenuity of the private sector" and its clear message that computer security solutions should be industry-led. The IT industry in the United States has been a global leader in the technology marketplace, and has contributed to the ascension of the United States as the leading nation transforming us into a Digital Planet. For a number of reasons, including its embrace of industry self-governance, the IT industry in the US has remained and creating jobs rich in opportunities and benefits.

III. Specific Issues

Aside from underscoring the importance of computer security, H.R. 2413 also addresses a series of sub-issues under the information security umbrella. Let me touch on a few.

IT Workforce

H.R. 2413 acknowledges a shortage of university students studying computer security and addresses the shortfall by establishing a new computer science fellowship program for graduate and undergraduate students studying computer security. ITAA supports this goal and tactic. ITAA long has been an outspoken organization on the impact of the shortage of IT workers—whether in computer security or any of the other IT occupations. Our groundbreaking studies on the IT workforce shortage—Help Wanted—have defined the debate and brought national attention to the need for new solutions to meet the current and projected shortages of IT workers. We fully support efforts by the Federal government to address the IT workforce shortage by developing efforts, such as the fellowship program outlined in the bill, to increase the number of IT skilled workers in the workforce.

The challenge to find InfoSec workers is enormous, because they frequently require additional training and education beyond what is normally achieved by IT workers. In addition, because many of the positions involving government InfoSec require US citizenship, using immigrants or outsourcing the projects to other countries is not an option.

Digital Signatures/Public Key Infrastructure (PKI)

The Computer Security Enhancement Act of 1999 also addresses a public key infrastructure (PKI) and digital signature technologies. Broadly, ITAA believes that PKI and digital signatures will be essential technological pieces of the bigger picture of information security. In the 105th Congress, ITAA strongly supported Senator Spencer Abraham's bill which was signed into law giving digital signatures the same legal recognition as handwritten signatures. In the 106th Congress, ITAA continues its support of a number of bills that intend to further enable the growth and acceptance of digital signatures.

IV. Areas to Address

While ITAA supports the broad themes outlined above, we would like to make a few suggestions to improve the legislation.

One of the major factors contributing to the dramatic growth of the IT industry in the United States has been the environment of industry self-governance and the role of marketplace competition. With a relatively hands-off policy of the Federal government on EC, enunciated most clearly in July, 1997, the IT industry has been able to innovate quickly to respond to the demands of the marketplace.

This environment has been particularly effective in the area of product development and standardization. When necessary, industry has come together to create standards bodies to address technology issues. In some cases, NIST has been an active participant in those agreements. However, developments in the marketplace and demands from customers often have led to "de facto" standards being established without burdensome technical rules or regulations.

In terms of H.R. 2413, ITAA has concerns with the use of the term "standards." Why? Broadly, the IT industry often sees standards as a snapshot of technology at a given moment, creating the risks that technology becomes frozen in place, or that government coalesces around the "wrong" standards.

The technologies underlying information security are in a critical stage of development. Companies across the IT industry spectrum are researching and developing software and hardware products that address information security through a variety of methods. Some are relying on software solutions to provide security. Others are exploring hardware answers, such as adding "security chips" to servers.

As noted author on business change Geoffrey Moore has described, technology often goes through a period best illustrated as a "tornado." During this period, companies are developing competing products to meet marketplace demands in a variety of ways. Gradually, the tornado will play out and market-driven industry leaders will emerge. The information security market is at this tornado stage, and efforts by the Federal government to establish standards would hinder the natural market forces from working.

What do we propose as a solution? While ITAA acknowledges the desire within the Federal government to achieve interoperability of products and systems through standard-setting efforts, we believe that the IT industry can address this simply by responding to the marketplace demand. Rather than establishing standards, we respectfully suggest the drafting of guidelines or best practices. With these as a resource, IT companies will develop product and services offerings that will meet the Federal government's need for greater information security.

As an example of this process developing in practice, let me offer you the Federal Electronic Commerce Coalition.

Recognizing a need for dialogue between the government and the private sector in the implementation of Electronic Commerce, ITAA co-founded last year, in conjunction with the Industry Advisory Council (IAC), the Federal Electronic

Commerce Coalition. The Coalition, currently consisting of eighteen trade associations and representing over 8,000 companies with subject matter expertise, has the objective of working directly with government in identifying "technology neutral" industry best practices in EC. The U.S. Department of Defense (DOD) and members of the coalition have recently created four Industry Process Teams (IPT) consisting of high-level industry and government representatives. Each team is focused on an important component of EC. These teams are backed up with working groups from both government and the Coalition's member companies who will work closely together to identify methods of overcoming barriers in the adoption of EC solutions between government and industry, government to government and industry to industry.

The Coalition is NOT a standards setting organization. The Coalition and the government feel that one size does not fit all and that companies and agencies should be free to adopt solutions that best fit their business needs. The critical issue is that these solutions be interoperable, that information be protected, that incentives for successful implementation be available and that trading partners across the spectrum be able to participate in EC without multiple systems, loss of flexibility and added expense.

The Coalition is working with many other government agencies in developing a cooperative process similar to that in place with DOD. The reception given to this concept of dialogue and cooperation has been encouraging and an exciting step in the growth of EC.

The past is littered with mandated standards that have failed. We cannot afford to take that path again. The technology is robust enough to allow custom solutions that allow interoperability. We look forward to the Federal Electronic Commerce Coalition becoming an important partner in the exploding growth of this new paradigm.

Conclusion

The U.S. and much of the world are building their economic house on an IT foundation. This is an extremely positive approach to take, delivering tangible benefits to a fast growing percentage of the world's population. As we build this house that reaches to a better, more prosperous and democratic future, we must be ever vigilant of cracks in this structure.

We applaud the Federal government's efforts to protect its house from these cracks. We stand behind the need for authentication through digital signatures and a public key infrastructure. We salute efforts to address the IT security workforce shortage. ITAA and the IT industry ask that you consider this—as well as our concerns raised above—as you debate the merits of H.R. 2413.

Thank you and I would be happy to answer any questions you may have.

ITAA

Harris N. Miller
President
Information Technology Association of America (ITAA)

Harris N. Miller became President of the Information Technology Association of America (ITAA) in 1995. Miller directs the day-to-day operations of the association and reports to the ITAA Board of Directors. ITAA is the largest and oldest information technology (IT) trade association, representing 11,000 software, services, internet, telecommunications, electronic commerce and systems integration companies. ITAA has grown more than 25% each year that Miller has been President.

Miller is also President of the World Information Technology and Services Alliance (WITSA), an "association of associations" representing 38 high tech trade groups around the world. Recently he has been named a member of the Board of Directors of ITT Educational Services, Inc., a publicly traded corporation.

Miller leads ITAA's public policy focus in other areas such as encryption, taxation, IT workforce shortage, intellectual property, telecommunications reform, Year 2000 date conversion, and business immigration. He has testified before Congress and state legislatures on numerous issues, and briefed federal, state, and local officials on issues critical to the IT industry. He was a member of the Board of Directors of the 1998 World Congress on Information Technology. He has written and spoken widely on a variety of high tech issues and has been published in various popular and academic journals -- among others, *IT Professional Magazine* published by the Institute of Electrical and Electronics Engineers, and *The World Today* published by The Royal Institute of International Affairs. He also serves on the advisory boards of The Alliance for Technology Education (TATE) and *IT Staffing Solutions*, a Harcourt Brace Professional Publication. He is a much sought after conference presenter both nationally and internationally.

Among many significant accomplishments during the past four years, Miller:

- Conceived the ground-breaking study, "Help Wanted: The IT Workforce at the Dawn of a New Century." Under his leadership, ITAA produced the National Information Technology Workforce Convocation, which brought together leaders from education, government, and industry to formulate partnerships and "best practices" to increase the quantity and quality of IT workers.
- Led the IT industry in supporting the passage of Telecommunications Act of 1996 and assuring statutory protections for IT companies.
- Directed the association's creation of a multifaceted Year 2000 Century Date Change Program. ITAA is widely recognized by both government and industry as the foremost trade association in the Year 2000 area. Played an instrumental role in formulating the International Year 2000 Cooperation Center (IY2KCC) and conducted the first global summit on the Year 2000 issue, bringing together representatives from over 130 nations.
- Helped achieve numerous legislative and regulatory victories for the Information Technology industry, including creation of the Foreign Sales Corporation credit for software exporters, extension of the Research & Education tax credit, an Internet tax moratorium, extension of the H1-B visa limit for highly skilled foreign professionals, and government procurement reform.
- Secured ITAA's position as IT industry sector coordinator for Critical Information Infrastructure Protection under Presidential Decision Directive 63.
- Appeared on numerous network and cable television programs, radio programs and has been quoted in virtually all major national news publications. These include CBS, NBC, CNN, CNBC, BBC, *Wall Street Journal, New York Times, Washington Post, Business Week, Financial Times, The Economist* and many more.

Prepared 8/99

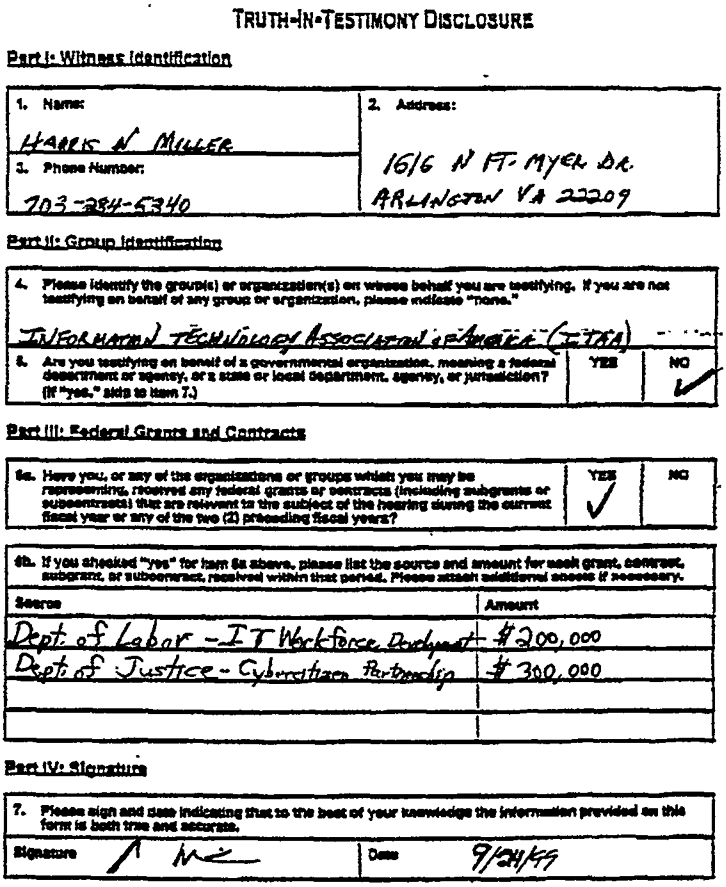
Miller has a broad range of additional public policy experience. Prior to joining ITAA, he was president of Immigration Services Associates, a government relations firm based in Washington, D.C. specializing in immigration issues. Concurrently, he acted as government relations director for Fragomen, Del Rey & Bernsen, P.C., a nationwide law firm specializing in immigration, and he operated his own government relations firm, Harris Miller & Associates, with clients in high tech, agriculture and banking.

In addition to private sector experience, Miller has many years of government service, including assignments as Legislative Director to former U.S. Sen. John A. Durkin (D-NH); Deputy Director, Congressional Relations, U.S. Office of Personnel Management; and Legislative Assistant, Subcommittee on Immigration, Refugees and International Law, Committee on the Judiciary, U.S. House of Representatives.

Miller is also active in professional and civic activities. He served as chairman of the Fairfax County, Virginia Democratic party for six years. He served as co-chair of the Virginia Opera Northern Virginia Finance Committee and was a member of the Virginia State Lottery Board. Miller was chairman of the American Heart Association, Northern Virginia Council; member, Virginia Governor's Commission on the Federal Funding of State Domestic Programs; and served on the board of the National Conference of Christians and Jews, National Capitol Area Region. Currently, he serves on the Boards of Directors of The National Center for Technology and the Law - George Mason University's Tech Center, and The Center for Innovative Leadership in Blacksburg, Virginia. Miller is Co-Chairman of the 1999 Wolf Trap Ball Corporate Committee, and was recently featured on the cover of *Association Management Magazine*. In June of 1999, Mr. Miller was the recipient of *Federal Computer Week's* "Federal 100 of 1999 Award", presented to "...executives from government, industry and academia found by an independent panel of judges to have had the greatest impact on the government systems community..."

Miller holds an undergraduate degree from the University of Pittsburgh and a graduate degree from Yale University.

Prepared 8/99



TRUTH-IN-TESTIMONY DISCLOSURE

Part I: Witness Identification

1. Name: HARRIS N. MILLER	2. Address: 1616 N FT. MYER DR. ARLINGTON VA 22209
3. Phone Number: 703-284-5340	

Part II: Group Identification

4. Please identify the group(s) or organization(s) on whose behalf you are testifying. If you are not testifying on behalf of any group or organization, please indicate "none."

INFORMATION TECHNOLOGY ASSOCIATION of AMERICA (ITAA)

	YES	NO
5. Are you testifying on behalf of a governmental organization, meaning a federal department or agency, or a state or local department, agency, or jurisdiction? (If "yes," skip to item 7.)		✓

Part III: Federal Grants and Contracts

	YES	NO
6a. Have you, or any of the organizations or groups which you may be representing, received any federal grants or contracts (including subgrants or subcontracts) that are relevant to the subject of the hearing during the current fiscal year or any of the two (2) preceding fiscal years?	✓	

6b. If you checked "yes" for item 6a above, please list the source and amount for each grant, contract, subgrant, or subcontract, received within that period. Please attach additional sheets if necessary.

Source	Amount
Dept. of Labor - IT Workforce Development	$200,000
Dept. of Justice - Cybercitizen Partnership	$300,000

Part IV: Signature

7. Please sign and date indicating that to the best of your knowledge the information provided on this form is both true and accurate.

Signature	Date 9/24/99

Chairwoman MORELLA. Thank you, Mr. Miller.
Now pleased to recognize Professor George Trubow.

STATEMENT OF GEORGE TRUBOW

Mr. TRUBOW. Madam Chairwoman, members of the Committee, and staff, good afternoon. I am George Trubow, Professor at the John Marshall Law School in Chicago and a member of the Computer Systems Security and Privacy Advisory Board.

I do want to point out that though I know I'm here because of my membership in that Committee, my testimony today cannot be said to represent the Committee, and that's because at our last meeting, 24-13, it wasn't on the agenda, and the board, as a whole, has not looked at it. Consequently, the opinions you hear today are largely my own, though I believe they're not out of joint with the majority of my colleagues and with those of the Chairman?

The main thrust of the bill, as stated in its purposes, is to reinforce the National Institute of Standards' ability to ensure security of unclassified information. And, indeed, the threats to the security and privacy information in electronic information systems has never been higher, and it will get worse, and I certainly support the provisions to increase the ability of NIST to deal with the security technologies.

The legislation directly address my board in section six, which Dr. Kammer has already referred to. That section would enlarge the role of the board and also provide some resources, which we have not had. The way it enlarges the role is by indicating that in section six, in the first paragraph of the section, that NIST shall solicit the recommendations of the Advisory Board regarding standards and guidelines being considered for submittal to the Secretary. I think that's fine.

That enlarges our role, because, currently, we independently identify issues and simply bring them to the attention of the board, and that's it. The change would require—I'm sorry, to the attention of NIST. The change would require NIST to ask us about its guidelines and standards that it plans to submit to the Secretary.

Now, the second sentence is the one that raises the problem for Dr. Kammer, and it raises one for the board as well. The second sentence says that "No standards or guidelines shall be submitted to the Secretary prior to the receipt by the Institute of the board's written recommendations."

We are an advisory board, and I think we've been effective in that role. We have never had the authority to interfere with the direction or management or programs of NIST, and we do not seek that authority. We believe that that first sentence strengthens our advisory role, however, and the third sentence, which says that the recommendations of the board shall accompany standards by changing the word "the" to "any," I agree with that one, as well, because if we choose to make recommendations, then I believe they should be sent along to the Secretary with the board's own recommendations.

Regarding resources, we're glad to have them. It helps us gather information upon which we base our recommendations, and it helps us to publicize information with respect to security and privacy.

The problem—the main problem I have with the bill deals with privacy, and I could go on and on, I guess, as you suspect, in a diatribe about privacy. On page three of my testimony, I kind of summed up my view for the Subcommittee when I said that each of us has got a host of electronic clones that reside in electronic information systems of the Government and the private sector, and those clones are manipulated, and, as a result, the persons they represent are affected. And, so I believe very, very much in protecting those clones.

And the bill doesn't deal with privacy. It deals with security. And I believe that privacy ought not be ignored, and I have an easy remedy. I would suggest to the Committee about half a dozen places where inserting the phrase "and privacy" will make me very happy. I think it will improve the bill, and in no way deter its attention and priority to security.

And let me be specific. On the draft of the bill that we have, in section two, the purposes of NIST, on line 21, on page two, I would insert "security and privacy" as one of the purposes for NIST activities.

Secondly, on page four of the bill, line five in section five, I would indicate that the evaluations and tests of information technology should assess "security and privacy" vulnerabilities.

Also, on the same page, in section six, where NIST is required to emphasize the development of technology neutral policy guidelines for computer security, I would insert "and privacy."

Additionally, I would, on page 8, on line 13, insert "and privacy" indicating that student supports at institutions of higher learning in computer security and privacy would be extremely useful.

I also support that section 10. I think the amount appropriated there is rather insignificant, however. We heard prior testimony about the need for security personnel, and my calculations are that if you figure a fellowship will provide about $10,000, we'd get 25 people the first year out of the appropriation and 50 the next, and I don't think that would make much of a indentation. We've got plenty of programs. We need to develop access to them.

The last place I would insert "and privacy" is on page 10, line 23, "to promote awareness of information security and privacy threats." If privacy is not kept before us, it will be ignored, and the major effort that I urge today is to keep privacy before us and to be sure that NIST keeps that as one of its priorities.

Thank you very much. I'll answer questions at your will.

[The statement of Mr. Trubow follows:]

SUBCOMMITTEE ON TECHNOLOGY,
THE COMMITTEE ON SCIENCE,
U.S. HOUSE OF REPRESENTATIVES
HEARINGS ON H.R. 2413

COMPUTER SYSTEMS SECURITY AND PRIVACY ADVISORY BOARD
STATEMENT OF GEORGE B. TRUBOW
September 30, 1999

The Subcommittee has invited me to testify on H.R. 2413, entitled "The Computer Security Enhancement Act Of 1999," which would amend the Computer Security Act of 1987 (CSA, PL 100-235). I am here as a member of the Computer Systems Security and Privacy Advisory Board (hereafter, the Board), established by the CSA.

The Board is composed of 12 members and a chairman; I was appointed to the Board September 10, 1997, as one of the four non-government, non-industry members. I am a professor at the John Marshall Law School of Chicago, and director of its Center for Information Technology and Privacy Law. As might be expected, my principal concern regarding the Board's mandate is with the matter of privacy.

The Board's chairman, Dr. Willis H. Ware, is out of the country and thus unable to be at this hearing, though I did have a brief exchange of e-mail with him before he departed. He previously testified before the Subcommittee on Technology on May 3, 1994, giving a detailed statement on the background and operations of the Board, and again on June 19, 1997, in connection with a proposal at that time for amendments to the CSA, which were not enacted. When the Board had its quarterly meeting earlier this month, H.R. 2413 was not on the table, so the Board has not considered the bill. Consequently, my statement today will be brief and for the most part reflects my own views.

The CSA charges the Board "to identify emerging managerial, technical, administrative and physical safeguard issues relative to computer system security and privacy, to advise the Bureau of Standards (sic, now the National Institute of Standards and Technology, hereafter "NIST") and the Secretary of Commerce on such matters, and to report its findings to the Secretary of Commerce, Director of OMB, Director of NSA, and appropriate committees of Congress." Let me first address H.R. 2413 as it directly affects the Board.

As indicated, H.R. 2413 amends the CSA, and Section 6 of the bill amends also the National Institute of Standards and Technology Act, by enlarging the role and functions of the Board, as follows:

> The Institute shall solicit the recommendations of the Computer Systems Security and Privacy Advisory Board...regarding

> standards and guidelines that are being considered for submittal to the Secretary.... *No standards or guidelines shall be submitted to the Secretary prior to the receipt by the Institute of the Board's written recommendations.* (emph. supp.) The recommendations of the Board shall accompany standards and guidelines submitted to the Secretary.

I believe the sentence in italics should be deleted from the bill. The Board meets only quarterly and has never had the authority to manage, approve or interfere with the work of NIST, nor does it seek such authority. We are named as an advisory board and should remain so, and I believe we have been effective in that role. I know that others on the Board share this view, and I take the liberty of quoting the chairman in an e-mail message of September 22, 1999, in the exchange I referred to earlier: "One thing you should be against is putting CSSPAB in the loop for approval of anything. We move too slowly to be in such a position. We can give advice and wisdom, but we should never be asked to consent." As stated, I share that opinion.

It is appropriate for the Board to be asked for its advice and wisdom, as provided in the first sentence of the language of H.R. 2413, quoted above. But, it should be for the Board to determine whether it has any advice or wisdom to offer regarding a proposed standard or guideline, and if it does then it is also appropriate that any recommendation be submitted to the Secretary. Accordingly, I would urge that the second sentence above be deleted, and that the word "the" which begins the third sentence, be changed to "any".

Section 6 of H.R. 2413 also contains a provision to authorize an appropriation to the Secretary of Commerce of $1,000,000 in FY 2000, and $1,030,00 in FY 2001, "to enable the (Board) 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." These resources would provide the Board with an expanded means of access to the information and evidence upon which to formulate its findings and recommendations as charged by the CSA and to disseminate the results of important studies and research within its purview. As a result, the Board's function and voice would be enhanced by the new resources and I believe that is a good result.

I believe it is especially important to give the Board the resources to enlarge its role and voice in the midst of our information age, which I often refer to as the "information revolution." The Board's role in monitoring and encouraging security system development supports a national goal of protecting sensitive government information from unauthorized access, alteration, loss or dissemination. By enlarging the Board's voice the benefits of its recommendations and the results of studies and research that it collects will be more readily shared with the private sector, which is certainly consistent with the bill's provisions generally authorizing and encouraging NIST's cooperation with the private sector. For instance, Section 12 charges the Department of Commerce to (1) promote widespread use of information technologies, (2) establish a clearinghouse to collect and disseminate information about information security threats, and (3) promote the commercial and private uses of encryption technologies.

Let me now address H.R. 2413 in another respect. It's title, "Computer Security Enhancement Act," signals its objective to enlarge NIST's activities in security system development. Historically, as between security and privacy, security has been first in line for NIST's resources, and a continued emphasis on security is certainly warranted, especially when risk to information security, both in the public and private sectors, is as widespread as it is today. Assaults on government and private sector information systems, whether by mischievous hackers or cyberterrorists, threaten the continued development and operation of the nation's information infrastructure. Accordingly, I certainly support the goal of H.R. 2413 to expand NIST's activities in developing and promoting the use of information system security technologies.

Attention to privacy, however, must not be overlooked. There is plenty of evidence of the constantly increasing collection and use of personal information in government and private sector information systems and data banks. What's more, personal information is collected in such fine detail that it provides dossiers and behavioral profiles of individuals in every segment of this nation's population. My view is that each of us has electronic clones --virtual personalities -- residing in those data banks and those clones are used to affect the real persons involved. The clones may be "processed" or manipulated for such activities as target-marketing, awarding or denying job opportunities or benefits of some kind, defaming the individual involved, committing credit card fraud, or engaging in the ultimate invasion of privacy, theft of identity. Whatever the context, the use of personal information confronts the right to privacy, and that right is basic to our fundamental right to freedom.

Security technologies protect privacy by guarding the access to and use of these information clones through policies and procedures that give individuals the ability to select and define the range of permissible "processing" of their clones. Thus, security and privacy are certainly intertwined, but there can be no privacy without the policies and procedures to guide the application of information system security measures. Therefore, I turn to the subject of privacy as addressed in H.R. 2413. In short, privacy is not addressed.

As I indicated earlier, NIST has focused on security, nor has the matter of privacy been a priority for the Board's attention, either. As the Board's chairman stated in his June, 1997, Congressional testimony, "In discharging its duties, the Board has interpreted its mission broadly, although to date, it has concentrated on security issues to the exclusion of personal privacy ones." That statement remains largely true today. But, though I support a continued priority for security concern, privacy must not be ignored, as it is in the current draft of H.R. 2413. I urge the Committee to remedy this oversight by making it clear that attention to privacy must be an integral part of security system development. I note here that at its last meeting, the Board itself moved to address privacy by establishing a task group to recommend a privacy agenda for the Board.

Finally, I address two other provisions of H.R. 2413. Section 10 authorizes an important new program, Computer Security Fellowships. The authorization of $250,000 for FY 2000 and $500,000 for FY 2001, could be regarded as minimal sums for something so important as educating specialists in the complex subject of computer and information system security. Even if all the funds were appropriated and used for fellowships, without diversion to administrative costs, it could be a long time before any appreciable growth in the supply of security specialists would be realized. At $10,000 per fellowship, not an unreasonable sum, only 25 students throughout the nation would benefit in the first year and 50 more in the second. I believe there is a serious shortage of security specialists; the security education programs are already here and we must enlarge access to them.

Section 14 of the bill authorizes $3 million in FY 2000 and $4 million in FY 2001 to supplement the NIST budget. I expect that testimony from NIST will discuss how much of the expanded program envisioned by H.R. 2413 could be accomplished with that addition appropriation, but I suspect not much of it.

That concludes my prepared testimony. I'll be pleased to answer questions to the best of my knowledge.

PROF. GEORGE B. TRUBOW
Director, Center for Information Technology and Privacy Law
The John Marshall Law School, Chicago, IL 60604-3907
Voice: 312-987-1445; Fax: 312-427-4280; E-Mail: 7trubow@jmls.edu

George B. Trubow is a graduate of the University of Michigan (A.B., J.D.) and, since 1976, Professor of Law at The John Marshall Law School where he teaches Information Law and Policy, Cyberspace Law, Privacy Law, and Computer Làw and directs the Center for Information Technology and Privacy Law.

Trubow practiced law in Kansas and Missouri from 1958-61, and in 1961 became assistant professor at John Marshall. In 1965, he was awarded a Congressional Fellowship with the American Political Science Association in Washington, D.C. From 1966-68, Trubow was deputy counsel to the U.S. Senate Judiciary Subcommittee on Judicial Machinery. In 1968 he became Executive Director of the Maryland Governor's Commission on the Administration of Justice, and he served on the U.S. Attorney General's Advisory Council on Law Enforcement Education. from '68 to '70.

In 1970, Trubow joined the Law Enforcement Assistance Administration, U.S. Department of Justice, where he served as Deputy Director of Law Enforcement Programs and Director of Inspection and Review, in charge of grant programs to the states and planning and program development for LEAA.

In 1974, Trubow became general counsel to the Committee on the Right to Privacy, Executive Office of the President, during the Ford Administration. The committee was concerned with the analysis and development of federal information and privacy law and policy; Trubow returned to John Marshall in 1976.

He is active in the ABA Section of Science and Technology; he was advisor to the National Comission on Uniform State Laws in drafting the Uniform State Information Practices Code and Reporter for the Uniform Criminal History Records Act. He was chair of the 1994 International Conference on Computers, Freedom and Privacy and is a member of the Bd. of Directors of the SEARCH Group, the national consortium for criminal justice information technology. He has been an advisor to the Office of Technology Assessment of the U.S. Congress, and to the National Research Council in Washington, D.C. He is a consultant on privacy to the U.S. Treasury Dept. Financial Fraud Institute, and a member of the Federal Computer Systems Security and Privacy Advisory Board.

Professor Trubow has written and spoken widely on the law of information technology, "Cyberspace," and privacy. He was law editor of IEEE's Software magazine;and his Center publishes a quarterly law review, The Journal of Computer and Information Law. Trubow is editor-in-chief of the three-volume treatise, "Privacy Law and Practice"(1987), and co-author of the casebook, "Privacy Law" (1992).

Chairwoman MORELLA. Thank you, Mr. Trubow. Thank you all very much.

I guess I'd start off right away picking up on what Mr. Trubow has said, Director Kammer. What do you think about the insertion of "and privacy" as well as the deletion that Mr. Trubow would suggest of no standards or guidelines should be submitted to the Secretary prior to going to the board and any other comments he may have?

And then I'm going to ask the rest of you if you want to comment on what you heard with regard to his specific suggestions.

Mr. Kammer?

Mr. KAMMER. With respect to the deletion in the section and the change of the word, I think that's a good way to go. I think that solves a problem and fulfills the intent that I took that the Committee make sure that the privacy board got an opportunity to comment.

With respect to the insertion of the word "privacy," I was able to find the bill finally there, and I think I saw where the last three went, and those made sense to me. I suspect the others would too, but I'd like to go back and look before I said for sure.

Chairwoman MORELLA. And we'll continue to look at it too.

I just wondered if Mr. Rhodes or Mr. Miller wanted to comment on any of those suggestions?

Mr. RHODES. Making certain that an advisory board has an advisory capacity is important in making certain that it doesn't become a blockade to getting any standard passed or any information up to the Secretary that's important. The addition of privacy with security is also a good suggestion, because privacy is becoming more and more important and will become more and more important as the average citizen does more and more business over the Internet. So, I would say those are good suggestions.

Chairwoman MORELLA. Mr. Miller?

Mr. MILLER. Ditto.

Chairwoman MORELLA. Good, good.

Mr. MILLER. You said keep it snappy.

Chairwoman MORELLA. I like it, right.

Mr. Rhodes, I like the suggestions that you made too. These are issues that, as you know, we have discussed before—accountability, implementation of the laws that we have, trying to clearly delineate the roles of the federal organizations and their responsibilities, and ranking the issues and all of those. We are going to try to do our darndest to incorporate what we can into this particular bill.

I think it would be appropriate, don't you?

Mr. RHODES. Yes, the reason I make these points is not to say that the bill is flawed; it's to say that we all have to understand that this is going to require wide collaboration. NIST is one organization, and I characterize them as an honest broker, and that's very important, but there was also a laundry list of other people who are associated with any discussions of public key infrastructure or cryptographic tools.

But, just as I said, cryptography is a very powerful tool in security and in privacy, but it can't solve negligence on the part of the people who implement it. If we establish an industry standard, we take an industry product, and then people take it out of the box and don't configure it properly, the industry standard is for naught.

So, the additional points that I'm making there are to—what we can get into the bill would be very helpful, but if we can't get any of those things into the bill, we need to understand that we're taking a very, very, very important first step in this bill as it is. Unfortunately, it's a journey of 1,000 miles.

Chairwoman MORELLA. It is indeed, and I guess nothing is so simple. Trying to incorporate what you have suggested into the bill could well have a dollar sign, and maybe not a dollar sign but may cost money, and I'm not sure whether that would be flowing from that $5 million that you mentioned, Director Kammer, or whether that would be an impediment.

Would you like to comment on the financial situation?

Mr. KAMMER. The additional $5 million in the—proposed for the 2000 budget is actually—sort of anticipates some of the instructions of the legislation. Two million dollars of it would go towards hiring 15 people who would be consultants to the rest of the Government—go around and assess people's systems and give them advice.

The other $3 million is to deal with creating technologies that benefit most Government agencies on one hand or security fixes that are unanticipated. I mean, by definition, we are going to encounter things that we didn't expect, and there will be times when money will have to be spent quickly in order to create a fix that everybody can use to protect their operating system.

Chairwoman MORELLA. Mr. Miller, how will the concepts that are included in this bill, 2413, benefit users of the Internet and consumers of information technology products?

And I want to mention that one of the reasons that some of our members on this side were not here is because they were with me before this at a demonstration, an Internet demonstration on what can be done with regard to pornography on the Internet as it affects young people. Evidently, there are a few demonstration programs—another area that interests me, too—but back to that question of this bill. Mr. Miller?

Mr. MILLER. Well, clearly, Madam Chair, survey after survey that we have done, and others have done, about the use of the Internet shows that the number one issue for consumers and business people and others is trust—trust on the Internet, trust that the people they're talking to or the people they want to be talking to——

We've all seen the cartoon from the New Yorker with the puppy sitting in front of the computer screen saying "The great thing about the Internet is you can be a dog on the Internet." Well, it's humorous and we all chuckle, but when you are passing sensitive information across the Internet, when you're doing research, when you're doing a business transaction, when you're buying a book on the Internet, you don't want to be doing business with a dog. You don't want to be sending information to a dog. You want to be sending information to the people you think you're going to be sending it to.

In addition, as Professor Trubow indicated, privacy is of huge concern to individuals using the Internet, and businesses using the

Internet. All of these are related to the question of information security, and information security depends a lot on leadership of organizations such as NIST particularly within the civilian agencies.

And I think that, again, comes back to the point I was making in my earlier statement. The world has changed a lot since 1987, and we saw an unfortunate incident when the Government went online about a year or so ago. As you may remember, the Social Security Administration was enabling individuals to access their social security records online, and sure enough, the first day I guess it was a reporter from the Washington Post went online, put in the appropriate information he needed to get it, and somebody else's records came up. So, right away, it blew the whole thing out of the water and made people skittish about it.

That has to be a major concern, and obviously information security specialists at NIST, while they can't guarantee they would have prevented that from happening, Dr. Kammer's group may have been able to work with that agency to make sure that wouldn't happen. So, that kind of leadership that's reflected in this bill is something that's very important to individual consumers and individual taxpayers.

Chairwoman MORELLA. Thank you, Mr. Miller.

I'm now going to recognize Mr. Gordon, but if you will excuse me, Mr. Bartlett will take over the Chair while I go to the Floor to speak on a piece of the legislation.

Thank you, and all members of the Subcommittee, with your permission, will submit questions to you for response, particularly as it pertains to this bill, some of the things we might do to touch it up so it can see passage imminently.

Thank you.

Mr. GORDON. Thank you, and let me thank the panel for some good suggestions in being part of trying to make this legislation as good as it can be.

I think that, to some extent, we're all a function of the experiences that we have, and we bring that to the table as we look at legislation. A few years ago, there was an effort to try to computerize the various election commissions in Tennessee. We have 95 different counties and a variety of cities within that. It seemed like a good idea. So, we were able to get that done and even provide a little bit of stipend to get that done.

What wound up happening is that, by and large, each county selected the—probably the least expensive or the first person that came in, and so there's no interoperability within the system, no way to communicate to the State, and we've got a mess. And years later, again, because of not wanting to get into additional expenses it hasn't fully been taken care of.

I have a concern that we could have a similar situation in that when you have agencies that have a federal, regional, state, a county, maybe a city office, that you may not even have operability within a department much less from department to department. This is one of my concerns and one of the reasons that we tried to put our section in.

And I'll start with you, Mr. Rhodes. Is this a—and I guess in the same thing in terms of security guidelines. We all know that there needs to be those security guidelines, but there are different levels of security, and do we really know that a particular product is going to provide that to us?

So, I guess my question, starting with you, Mr. Rhodes, is do we need to have some guidance here, and is there a better way to do it than we're trying to put forth in this legislation?

Mr. RHODES. Yes, we do need the guidance. I don't think there's—as long as the intent of the legislation is to get guidance by collaboration, that's going to be the correct answer.

The concern that I have is that if we have a series of products that are sitting on the table, and we say these products are considered secure by the Government, I, as the buyer of those products, don't really know what my risk is. I haven't assessed my risk.

That's the concern that I have is making certain that the people who are buying the product or applying the guideline or something like that, as long as the guidelines also let me know that at this level of risk this guidance applies; at this level of risk, this guidance applies; at this level of risk, this guidance applies. But I, as the follower of the guideline, have to understand how I'm supposed to assess my risk.

Dr. Kammer and I were talking just earlier that it's not really up to the NIST or industry or anyone like that to look at an individual agency and say, "Your risk is X." One aspect of this would probably be helpful if there were guidelines on risk assessment, on how to understand what my vulnerability is and what the value of the assets on that I'm trying to protect. If there were either guidance published or a call for guidance to be published on risk assessment, that would be very helpful as well.

Mr. GORDON. Well, if an individual or a purchasing agent couldn't figure out what risk they need, they certainly couldn't' figure out what product would provide it.

Mr. RHODES. Absolutely.

Mr. GORDON. So, what our objective is, is to try to have these minimum standards so that hopefully a variety of commercial products will be developed, will be on the shelf, and then hopefully there will be the competition to get the price down and the service up.

Mr. RHODES. Good.

Mr. GORDON. Did anyone else want to have any suggestion as to concerns about this continuity of interoperability?

Mr. MILLER. A couple of comments, Mr. Gordon. Number one, one hopes in the late 1990's that would not happen again, because obviously people are much more sensitive to interoperability or the old stove-pipe mentality about computer systems, we hope is almost dead, if it's not totally dead. But it's hard to eliminate the practices.

But let me try to quickly summarize what seemed to be two contradictory elements, but I don't think in fact are contradictory. On the one hand, industry and this panel have agreed, and I think your Subcommittee agrees, that we want to promote competition in the private sector; we want to promote innovation in the private sector. And the word "standards" to industry, at least, connotes the possible negative result that you take a snapshot at one particular point in technology, and you say, "This is it," and this becomes the standard, and everybody's got to work to that. And if you do that, the concern is that you then freeze innovation, you freeze out of the marketplace, competition. So, that's why industry is so concerned about the word "standard", as opposed to guidelines or procedures or collaborative action.

On the other hand, industry is not unmindful of the fact that the customer doesn't want to be put in a situation you described where either making purchases that don't work with other purchases or just making purchases with no information and not understanding the capacity or capability, whether it really does provide information security.

So, I think what you're seeing right now is the customers are starting to move in the right direction. One example is the banking industry announced a couple of months ago that they're actually putting together a collaborative effort to begin to, and I'll use the word "generically test" products and procedures out there in the marketplace so that they can in a sense tell banking industry people and executives who are making IT purchases what are the products and what kind of performance do they really give.

I don't think this organization intends in any way to again set standards, but they do want to perform the kind of evaluation that I think Mr. Rhodes is referring to so that a CIO of a bank would have some intelligent, objective information on which to base a decision whether to buy a particular IT product or service other than what the salesperson of that company is telling him or her.

So, I think what you're seeing is the customers are going to be working with the people in industry who create the products so that even though there aren't going to be standards, there are going to be objective measures out there that people can look to before making buying decisions.

Mr. GORDON. Well, I think—you know, it has been explained I think informally, and if it takes explaining it formally, I will. The term "standards" is a term of art that allows basically NIST to have this function without getting into jurisdictional problems here in this Congress.

Now, as a practical matter, if you think something needs to be done, then it's going to be more likely to get it done in a streamlined method dealing with maybe one committee here rather than a variety of committees. So, again, I think that we all know that, but now there will be no misunderstanding.

Mr. TRUBOW. Mr. Gordon?

Mr. GORDON. Yes?

Mr. TRUBOW. Could I make a comment about interoperability?

Mr. GORDON. Sure.

Mr. TRUBOW. Again, from the privacy perspective, interoperability of course increases the privacy threat, because when you begin hooking up and connecting a variety of databases, you increase the privacy threat. As has been said before and I indicated in my statement, you can't have privacy without security, and therefore good security is increasingly important in an environment of interoperability. And I want to make that quite clear.

Mr. GORDON. Oh, sure. There's something of a matrix in that at different levels you'll have different means of or different standards—boy, that's a bad term, isn't it—different levels of security.

But the ultimate security is only you know the code, but it's not going to help you if you can't talk to somebody down the street.

Mr. TRUBOW. Let me share this experience with you. Back in 1974, 1976, I was Counsel to the Privacy Committee in the Executive Office of the President that had been established right after the Watergate affair. And at that time Ruth Davis was Director of then National Bureau of Standards, and I asked Director Davis if she could develop a series of security levels—minimum, medium, maximum, one, two, three—and give us some standards for achieving each of those levels.

She did some work on it then and reported to me that she could not do that; that she could discuss risk assessment and discuss how to go about assessing vulnerabilities but could not assign categories or levels.

Now, technology is not my strong point, and I would hope that we have advanced somewhat since then, although I expect it will continue to be a very, very difficult task for NIST to undertake.

Mr. GORDON. It probably will be. That may also be a function of someone not wanting to take responsibility in that if some level was broken that they said it was okay, and then it wasn't. So, they're the ones that are at fault.

One last quick question. Part of this legislation also sets up a national policy panel for digital signatures, which is, again, a public-private sector gathering and consultation to try to look to the future to see what are going to be potential problems and solutions. Mr. Rhodes, what are—there are some criticisms this might mirror other ongoing efforts. What is your opinion as to that?

Mr. RHODES. Well, it would depend on who's involved in the panel, of course. I mean, the current struggle that I see regarding not just privacy issues but security in general is making certain that law enforcement is addressed—or the concerns of law enforcement and the concerns of national security are addressed. If all parties are brought to the table, if this panel is encompassing of both industry and Government, then it should be successful.

The concern that I have is that making certain that the panel is inclusive, because right now there are many exclusive discussions taking place and not much verbal interoperability between those discussions.

Mr. GORDON. The hope would be that rather than having to wait for a train wreck, it's sort of the signal up ahead that says the train wreck is getting ready to come, and so get ready.

Mr. RHODES. Well, it is here. I mean, the requirement is here now. You were talking about in your own State with the voter system, but even on things as simple as getting store coupons over the Internet, you hear from the companies that issue the coupons that 40 percent of the coupons that are redeemed are forged, because people download them on the Internet, load them into their Photoshop program and modify the value or the date or something like that. So, it's here now to try and have integrity.

Mr. GORDON. Well, I think also you have a situation—I guess you have regular time, then you have dog time, and then you're going to have Internet time.

Mr. RHODES. Right.

Mr. GORDON. And, so whatever we're thinking about today and as bright as you are, within 6 months there's going to be another problem or opportunity that you really didn't anticipate, and it's trying to stay somewhat ahead.

Does anyone else want to make a comment concerning——

Mr. MILLER. Just one quick suggestion, Mr. Gordon. You might think about changing it from digital signatures to a more broad term of electronic authentication, because digital signatures still carries the connotation of a particular type of technology. It's technology-specific, and, obviously, again, in Internet time, people are looking at biometric identification and other types of identification which are not the traditional digital signatures. So, it's something you can think about.

Mr. GORDON. Right.

Well, again, my thanks to the panel for their cooperation, attendance, and good advice.

Mr. BARTLETT [presiding]. Thank you very much.

In a former life, I worked 8 years for IBM. But in spite of that, by today's standards, I'm relatively computer illiterate. And I just want to ask you a question as an interested observer but not an expert in the area.

There's some things that appear to me to be essentially mutually exclusive. On the one hand, you say that essential to security in the use of computers is trust, and I would suggest that you can't trust bad guys. Secondly, you have two interested I think or perhaps mutually exclusive—one is you want interoperability, and to be useful, the net must be very open, and yet you want privacy.

And my question is, don't we have an essentially insolvable problem that you can't have security if essential to that is trust, because you can't trust bad guys? And ultimately you can't have interoperability and openness and still have privacy? I know that we are doing a pretty good job of meeting these goals, but won't we always be kind of running behind the bad guys simply because of the mutual—essential mutually exclusiveness of these two objectives?

Mr. Kammer?

Mr. KAMMER. Yes, sir. We can't make things perfect. We can make them better, and that's sort of the context in which I'll answer the question. But don't trust bad guys. On the other hand, you can trust NIST, and we are evaluating computer security products, and we're characterizing them, and we're sharing that with the public and with other Federal agencies.

And in addition to that, your question about interoperability versus privacy. It's possible using cryptography to confer confidentiality upon yourself and at the same time be interoperable with other people that you've predetermined that you will share your information.

Mr. BARTLETT. But then you sacrifice openness, don't you?

Mr. KAMMER. Yes, it's a tradeoff. I don't think most people that want to sell a product are going to make their web sites confidential; that's illogical. Obviously, you want more—the more foot traffic the better, right? It's the same on the Internet. And I think you're going to find that confidentiality is going to be more reserved for business transactions where you only want to share your business with the person with whom you intended to have the transaction.

And it's possible to have mixed systems where you're sailing along on the Internet, you're completely in the open, you're not using cryptography, and then you invoke it for a particular activity, because you want that concealed from others. You'd like to be in private conditions under that—in that place, and then go back into the open again.

Mr. BARTLETT. But you would agree that the specialists who are trying to provide computer security will probably never be out of a job?

Mr. KAMMER. Never. The technology is going at the speed of light.

Mr. BARTLETT. Professor?

Mr. TRUBOW. Mr. Bartlett, there is a tension, but I don't believe that our society is ready for an open society in the sense of let it all hang out. And the important aspect of privacy is that it emphasizes the right of the individual to decide how open he wants to be about sensitive personal information.

Now, of course, that's a constant balance and negotiation that goes on between the individual and those people that he interacts with. How much am I going to, how much am I required to?

It's working out pretty well when the privacy interest is recognized, and I think that though there's a tension that we can work those out.

Mr. BARTLETT. Mr. Miller?

Mr. MILLER. I guess I don't agree with at least the second tension you suggested, Mr. Chairman, and that is the one between interoperability and privacy. Interoperability means to me that you have a highway that goes everywhere, anywhere, all the time, and there aren't special blocks, and it's not like the old railroads which had different gauges or the European roads——

Mr. BARTLETT. But if you're on that highway, aren't you then visible and haven't you given up privacy?

Mr. MILLER. You're visible, but then the question is what's on the highway, and you have some suggestions—some alternatives here, which I think Dr. Kammer suggested. You can travel in an armored car, which has a lot of very, very thick walls. It may go a little slower, you may need to take some special routes, but it's going to be real tough for the bad guys or other people to break into that.

On the other hand, you may want to have a sporty roadster that goes real fast and can go anywhere, but it's pretty easy for people to get at it. And that depends again on the technology. If you're sending medical privacy information over the Internet, you're going to want to be real sure that it's in an armored car, as armored as the IBM and RSA and EDS, et cetera, experts can make it. If you're just, as Dr. Kammer suggested, have an open web site and you want as many people to come there as possible, and you figure you're going to get—somebody's going to buy something once in awhile and forget to pay for it, you're willing to take that risk.

So, I think that it's not in attention. I think it's levels of sophistication that you want to bring to protecting that automobile or that transport mechanism. Again, clearly encryption is the important variable here, and that's why the decision of the Administration, under Congressional pressure recently, to change the encryption policy is such a positive step for electronic commerce.

Mr. BARTLETT. Encryption is the armored car you were talking about?

Mr. MILLER. The level of armoring it. And I'll just say the work that NIST is doing now to develop the advanced encryption standard, the decision that the Administration made to allow this, is what allows people to be never 100 percent confident, but fairly confident, that their information is either very highly protected or know that it's not really very well protected.

And, also, the other issue which relates to Mr. Gordon's provision is authentication. You want to make sure that people are really sending you the information, and it's not just an armored car, but it's really coming from the person who you think is sending the armored car. You don't want to open it up, think you've got correct information because it's been so well protected, but in fact it came from somebody you didn't expect to get it from.

Mr. BARTLETT. Which brings me to another tension. I have the privilege also of serving on the Armed Services Committee, and, as you know, we're very much concerned about encryption and not having the key for it. And the tension there is between the right of privacy and the right of the American people to be secure that we're not going to be giving away secrets that can be used to our detriment by a potential enemy.

That's just one other tension, and it's very difficult to know where to come down on the right side of that. Personally, I'd rather err on the side of being careful. We can make mistakes in the Science Committee, and sometimes we do, and we can come back and correct them next year. On the Armed Services Committee, you may not have a chance to come back if you screw up bad, and so I'm prone to err on the side of being careful there.

Mr. Rhodes, do you have any comments on these tensions?

Mr. RHODES. Just as we were discussing levels, interoperability is a generic term that also has levels. If you and I want to have a closed communication between us, and I wrap my message in some secured package and send it to you, and you open that package and it's correct, and you verified me and I verified you, then you and I truly are interoperable at that point. We're interoperable at many levels in terms of the hash on it, the cryptography, everything that's associated with it. It's a matter of do I want to be interoperable with everybody all the time or do I want to be interoperable with just a few people on a particular transaction. That's the distinction. You can actually I think have very, very strong privacy and still be interoperable, it's just not—you're not interoperable with the world.

And another point that I have to stress is that we have to make certain that the armored car is not taking a message from somebody living in a cardboard box to somebody who's sleeping on a park bench. Because those two systems at the end of that very secure transaction can't be like swiss cheese. I mean they have to be secured as well. That means you have to have a strong operating system, strong applications, strong authentication at the user level to get onto the system. It's not just at this transaction level between yourself and myself. If we're going to operate with an armored car, then we have to be in our own bunkers.

Mr. BARTLETT. Problems 10 years ago we never dreamed we'd have.

Mr. RHODES. No, sir.

Mr. BARTLETT. Mr. Gordon, you have additional comments or questions?

Well, I want to thank the panel very much for your testimony. Thank you for your willingness to work with us to draft legislation that's going to be most effective.

The Committee will stand in adjournment.

[Whereupon, at 2:50 p.m., the Subcommittee was adjourned.]

I

106TH CONGRESS
1ST SESSION

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.

IN THE HOUSE OF REPRESENTATIVES

JULY 1, 1999

Mr. SENSENBRENNER (for himself, Mr. GORDON, and Mrs. MORELLA) introduced the following bill; which was referred to the Committee on Science

---

A BILL

To amend the National Institute of Standards and Technology Act to enhance the ability of the National Institute of Standards and Technology to improve computer security, and for other purposes.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Security Enhancement Act of 1999".

SEC. 2. FINDINGS AND PURPOSES.

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

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

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

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

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

(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), (7), and (8), respectively; and

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

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

SEC. 4. SECURITY OF FEDERAL COMPUTERS AND NETWORKS.

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

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

"(6) to perform evaluations and tests of—

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

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

SEC. 5. COMPUTER SECURITY IMPLEMENTATION.

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

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

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

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

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

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

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

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

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

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

"(2) There are authorized to be appropriated to the Secretary $1,000,000 for fiscal year 2000 and $1,030,000 for fiscal year 2001 to enable the Computer System Security and Privacy Advisory Board, established by section 21, to identify emerging issues related to computer security, privacy, and cryptography and to convene public meetings on those subjects, receive presentations, and publish reports, digests, and summaries for public distribution on those subjects.".

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

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

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

SEC. 8. MISCELLANEOUS AMENDMENTS.

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

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

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

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

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

SEC. 9. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.

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

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

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

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

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

SEC. 10. COMPUTER SECURITY FELLOWSHIP PROGRAM.

There are authorized to be appropriated to the Secretary of Commerce $250,000 for fiscal year 2000 and $500,000 for fiscal year 2001 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 2000, to remain available until expended, for carrying out this section.

SEC. 12. PROMOTION OF NATIONAL INFORMATION SECURITY.

The Under Secretary of Commerce for Technology shall—

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

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

(3) promote the development of the national, standards-based infrastructure needed to support

commercial and private uses of encryption technologies for confidentiality and authentication.

SEC. 13. ELECTRONIC AUTHENTICATION INFRASTRUCTURE.

(a) ELECTRONIC AUTHENTICATION INFRASTRUCTURE.—

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

(A) sufficiently 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) minimum 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 coordination with the efforts of the National Policy Panel for Digital Signatures under subsection (e).

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

(b) VALIDATION OF PRODUCTS.—Not later than 1 year 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) ELECTRONIC CERTIFICATION AND MANAGEMENT SYSTEMS.—

(1) CRITERIA.—Not later than 1 year after the date of the enactment of this Act, the Director shall establish minimum technical criteria for the use by Federal agencies of electronic certification and management systems.

(2) EVALUATION.—The Director shall establish a program for evaluating the conformance with the criteria established under paragraph (1) of electronic certification and management systems, 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 systems evaluated as conforming to the criteria 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;

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

(3) an evaluation of the extent to which Federal agencies' electronic certification and management systems conform to the criteria established under subsection (c)(1);

(4) the list described in subsection (c)(3); and

(5) evaluations made under subsection (b).

(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 sig-

nature 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 systems" 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 $3,000,000 for fiscal year 2000 and $4,000,000 for fiscal year 2001, 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.

O

SUBCOMMITTEE ON TECHNOLOGY

HEARING ON H.R. 2413, THE COMPUTER SECURITY ENHANCEMENT ACT OF 1999

Opening Statement of Congresswoman Debbie Stabenow
of the 8th District, State of Michigan

September 30, 1999

Madame Chairwoman, Ranking Member Barcia, I appreciate the Subcommittee's continued attention to computer security here today. I look forward to learning more about how H.R. 2413 would update the computer security efforts initiated by the Computer Security Act of 1987.

The Subcommittee has addressed computer security concerns earlier this Congress, and given the pace of technological development, a review of the 1987 law is in order. The Internet, e-mail, and the speed of computers have not only increased in use over the last decade, but increase in capability year-to-year and even month-to-month. At the same time this technology has buoyed our economy and improved our quality of life, technology can also be used for destructive purposes. It is an eye-opening fact that the Department of Defense endured 250,000 hacker attempts last year alone. The threat of cyber-attack makes it crucial that the roles of the National Institute of Standards and Technology and other agencies must be clear if we are to effectively protect our computer systems.

Madame Chairwoman, I also think it is important that this bill incorporates provisions regarding digital signatures and electronic transactions. It is essential that the government acts in a predictable way in regard to commerce on the Internet, and this bill will help move that process forward. I appreciate the time and expertise of our witnesses, and again thank the Subcommittee leadership for their attention to this issue.

Statement On

The Review of the Computer Security Enhancement Act of 1999
to the

United States House of Representatives
Technology Subcommittee of the
Committee on Science

By

Charles W. Talley
Director, Information Engineering Center
OAO Corporation
Greenbelt, MD 20770

September 30, 1999

Introduction

Madam Chairwoman and members of the subcommittee, it is a great privilege to have the opportunity to appear before you today. As Director, of OAO Corporation's Information Engineering Center and as a IT Committee Chairman for the High Technology Council of Maryland (HTCM), I welcome this opportunity to work with you on the critically important task of improving the security of computer systems. With over 4300 people developing IT systems worldwide, OAO Corporation is the largest IT Minority Business Enterprise in the state of Maryland. The HTCM is a strong and active member of the IT industry, representing a synergistic joining of leaders and technical experts from the state government, educational institutions and all components of the IT industry throughout Maryland. Both OAO and the HTCM have consistently been forward thinking and innovative leaders in technology development and I would like to share with you the results from our review of the Computer Security Enhancement Act of 1999.

The Need to Update the Computer Security Act of 1987

Through my membership in the HTCM and a number of other state and national IT organizations, I interact on a continuing basis with a wide range of industry experts. The people that I have spoken with all wholeheartedly applaud your committee's efforts and diligence in enhancing the computer security posture of the civilian government agencies. OAO Corporation and the other members of the IT industry work in partnership with civilian government agencies on a daily basis to develop and implement computer systems that are often critical to the functioning, security and prosperity of this nation. Because of this, we recognize the necessity and the imperative to constantly find new ways to guard against vulnerabilities in new technologies and to guard against new ways of exploiting existing technologies. The risks associated with computer systems are well documented. Almost every day's newspaper contains stories of new attacks on government or commercial computer systems. The incident that I remember most was an investigation that I assisted with involving a well-known and respected research center that had its computer system broken into. There was no apparent damage, but unbeknownst to them the attacker changed a single number used in a formula. This change effected the results of computations and the decisions that were made for follow-on research were made based on those flawed results. It was almost a year before the change was detected and most of the work completed during that period had to be discarded because it would be too expensive to recreate and rerun the true research data. The increased proliferation of networked computer systems and the corresponding increase in the use of the Internet and web technologies have supported a monumental increase in the computing power of most government and commercial organizations but, these same technologies have made an attack such as the one I just described even more likely to occur today and in some cases even easier to perpetrate. For the first time in our history small mistakes, such a single error in configuring a Web server, can expose thousands or even millions of private data/records (such as credit card, medical or financial) to being captured, changed or displayed to unauthorized individuals worldwide in a matter of seconds. It is for these reasons that it is important for this committee to update the Computer Security Act of 1987.

The Industry View of HR 2413

I view the Computer Security Enhancement Act of 1999 as a positive step forward in the on-going effort to provide effective, but not stifling, computer security policy and guidance. It is an important, but extremely difficult process to establish an open and interoperable computing environment that will support the free and open exchange of ideas, services and information, while at the same time protecting the integrity, security and privacy of information. I believe that this Act strikes a balance by providing clear and concise security guidance while allowing the flexibility necessary to meet future requirements. There are many outstanding features in this Act, but in particular I am happy to see that the Act promotes and encourages the acquisition of Commercial-of-the-shelf (COTS) products. This will, in many cases, allow industry to continue providing high quality products while meeting the much shorter times schedule of today's computer projects and to accomplish this at a significantly lower cost.

Another valuable feature of the Computer Security Enhancement Act of 1999 is its emphases on the future as well as the present. OAO Corporation is sponsoring four graduate level students in computer security study at Carnegie Mellon University and we will be pleased to be working alongside the NIST's fellowship program as we all work toward our mutual goal of building the computer security expertise that will be so critical in the future. Your establishment of the National Panel for Digital Signatures, the study of PKI and the establishment of a clearinghouse of security information will all provide central focal points of expertise that will move the study of computer security rapidly forward.

The Need for an Interoperable Infrastructure to Facilitate E-commerce and How Can Authentication be Assured Through the Widespread use of E-signatures

The past few years have seen a tremendous growth in the number, complexity and dollar value of e-commerce transactions that are occurring, while at the same time the technologies used to support the growth of e-commerce have added a whole new dimension to the risks associated providing these products and services. Most of the billions of dollars currently being passed through e-commerce have been for "individual-to-business" commerce, but the next few years will see a rapid and dramatic increase of the use of e-commerce for "business-to-business" and "individual-to-government" purposes. Under the government's current environment of reduced spending and personnel, the use of an interoperable infrastructure to facilitate e-commerce technology will play an increasingly important, and in fact crucial, role in the government's ability to continue providing effective and efficient services to individuals, as well as to transact government business with commercial companies and state/local agencies. However, e-commerce will only be effective in meeting these demands if it can be implemented in such a way as to be: standardized, open structured, easy-to-use, cost effective and verifiably secure in both data integrity and privacy of information. OAO Corporation and the HTCM will continue to work with government to design, develop and implement systems that meet all of these e-commerce requirements. But, it is certain that without a standardized and verifiable security structure based on realistic encryption policy and digital signatures/certificates that can be used to authenticate both content and origin, individuals and businesses will be unwilling to expose their important, and often private, data/resources to the risk of interception and modification by unauthorized individuals or groups. Much progress has been made recently in the areas of digital signatures, certificates and Public Key Infrastructure (PKI). Your establishment of a National Panel for Digital Signatures, study of PKI and establishment of a clearinghouse of security information will provide central focal points of expertise that will move the practice of computer security forward even more rapidly.

CONCLUSION

Thank you, Madame Chairwoman and members of the Committee for your leadership in promoting computer security in today's ever changing and increasingly more complex technological environment. It is interesting to note that the Computer Security Act of 1987 updated a security law that was established 86 years before, in 1901. The Computer Security Enhancement Act of 1999 is necessitated by technology changes that occurred in 12 years and the next update will probably be necessary in only a few years. The power of today's computers, software, networks and global e-commerce are effective tools in meeting our mutual goals of increasing productivity with less resources. However, at the same time the risk associated with these tools and technologies are daily realities in the work being accomplished by the partnership of government and contractors. As the public continues to demand ever better and more effective services and wider access to information from civilian government agencies, it is critical that we have efficient, usable, cost effective computer standards and policies to enable us to mitigate the risk associated with meeting these demands. We look forward to working with you as the "Computer Security Enhancement Act of 1999" progresses.

Charles W. Talley
OAO Corporation
7500 Greenway Center Dr.
Greenbelt, MD
301 220-7148, ctalley@oao.com

SUMMARY OF QUALIFICATIONS

- 33 years technical, managerial and business development experience in the IT Industry, to include Computer Systems Security, Business Area Analysis (BAA), Business Process Reengineering (BPR), Business and Scientific Applications Development and Business/Marketing Development through the growth of existing and acquisition of new contracts.

- 18 years IT program and project management experience involving leading teams of up to 300 people in the successful completion of large-scale, complex government and commercial contracts across multi-state areas.

- Business development experience includes: development and implementation of strategic and operational marketing plans that have resulted on annual revenues in excess of $20M, presentations to large groups and individual decision makers that have led to the winning of multimillion dollar contracts, plus leading the marketing efforts of 3 Group Managers and multiple Task Leaders to consistently exceed corporate revenue goals. Proposal development experience includes leading and writing management, technical and cost volumes.

EDUCATION

MA Computer Resource and Information Management, Webster University, 1995
BS in Computer Studies, University of Maryland, 1992
BS Business Management, University of Maryland, 1988

SECURITY CLEARANCES

TS- SCI Updated by DISCO in Apr. 96, NSA Polygraph passed Mar 10, 1994

CHRONOLOGICAL SUMMARY OF EMPLOYMENT

Employment Dates:	Aug. 95 - Present:
Company & Title:	OAO Corporation, Greenbelt, MD. Director, Information Engineering Center / Senior Group Manager
Supervisor:	Mr. Bruce U. Hair (VP, Information Technology Division)

Provides oversight, planning and coordination for large IT contracts valued at up to $76M, providing information technology support services to government agencies (General Services Administration, Environmental Protection Agency, US Departments of Labor, Education, Commerce, Defense, Transportation, and Agriculture; the National

Institutes of Health; the U.S. Bureau of Prisons, and the National Institute for Standards and Technology including staffing of over 300 employees at widely spread locations in three states and the District of Washington. Manages multiple complex IT tasks using "best practice" techniques such as Earned Value Analysis, automated cost and schedule estimating and Risk Mitigation through Measurements of Effectiveness. Works closely with customers, and program and project managers to ensure that quality services are delivered on time and within or under budget.

Ensures quality of deliverable products and services through direct management of the verification and validation (V&V), testing, Quality Assurance (QA) and Configuration Management (CM) functions. Coordinates ~~operational issues with corporate management~~ to ensure adequate resources are available, as needed, to contract managers; and provides technology guidance to all projects. Provides customers with technical solutions for information engineering, applications software development and maintenance, telecommunications service requirements, and quality assurance. Supports all strategic planning and major business development initiatives. Developed task order proposals, work plans, and budgets; and handled all phases of personnel actions on multiple task orders.

Develops and implements computer security programs for complex computer systems operating in widely dispersed locations and using state-of-the-art technologies. Analyzes security risks and implements risk mitigation plans based on the roles, functional process and technical infrastructure of specific program requirements.

Plans, organizes, staffs and leads large scale Information Engineering (IE) tasks involving the Business Area Analysis, Process Reengineering/Improvement and System Development efforts necessary to implement complex computer application systems. Supervises teams of up to 175 people with diverse technical skills to accomplish multiple concurrent objectives. Oversees the operation of the Information Engineering Center (IEC), to include facilitation of Group Working Sessions using automated tools sets such as Oracle CASE Tools (Designer/Developer 2000), GSwin, BPwin and ERwin, to develop IDEF compliant Business Process and Data Models. Works with customers and system users to develop functional, hardware, and software requirements leading to full Software Development Life Cycle (SDLC) for multi-functional automated systems in the Oracle RDBMS in UNIX and Windows NT environments.

Responsible for marketing, developing and leading major Information Engineering (IE) programs and projects that provide Information Technology (IT) Services throughout Washington DC, Maryland, Virginia and North Carolina. Specializes in providing total solutions to IT problems through business area analysis, process reengineering, technical infrastructure design, and information systems implementation. Developed and implemented Strategic Plans that have exceeded corporate goals. Directs the daily operations of Group Managers and Task Leaders as they expand their business base and manage on-going tasks to exceed customer expectations. Supervises teams with diverse technical skills to accomplish multiple concurrent objectives. Leads the day-to-day operations of the Information Engineering Center (IEC). Serves as CIO of the

Information Technology Division, setting standards, controlling the infrastructure design and approving the purchase of computer equipment in support of over 400 users at four locations.

Employment Dates: Sep. 92 - Aug. 95
Company & Title: VSE Corporation,
Alexandria. VA
Department Manager / Production Manager
Supervisor: Steve Mitton

Managed the Information Technology Department in the successful accomplishment of three year, multimillion dollar computer applications for both government and commercial markets. Technical Manager of computer systems analysis, programming and documentation processes necessary for production of computer software. Conducted efficient customer support and help desk operation for existing application software systems. Supervised daily operation of an office consisting of a variety of technical specialties including section supervisors, team leaders, systems analyst, programmers and other specialists. Supervised and performed systems analysis during evaluation and implementation of major computer projects to support organization's production and marketing efforts. Configuration Managed software development in INFORMIX 4GL, ORACLE and C programming languages for a variety of UNIX and MS-DOS platforms. Designed and supervised the implementation of database systems for INFORMIX and ORACLE RDBMS. Developed project requirements and plans for achieving organizational long and short-term goals.

Employment Dates: Aug. 90 - Jun. 92
Company & Title: US Army Training Support Activity, Europe
Frankfurt, Germany
Info. Mgt. Officer / Project Manager
Supervisor: Jerre F. Spruill

Project Manager for the European Visual Modification (VISMOD) program that designed and implemented computerized and mechanical training devices for US Army Europe. Systems and Network Administrator for local area network installed on distributed Intel Minicomputers, running applications under the UNIX operating system. Supervisor of the Electronics Production and Repair Section. In his absence, acted as Chief of US Army Training Support Activity Europe, directing the daily activities of eight supervisors and 137 workers. Sr. Programmer and Database Administrator for a large inventory and financial tracking system. ADP/Network Security Manager for the organization and Asst. Security Manager for the military installation.

Employment Dates: Sep. 89 - Aug. 90
Company & Title: US Army Printing and Publication Center, Europe
Frankfurt, Germany
Special Assistant to the Dir. / Deputy Security Manager,

Supervisor: Stafford C. Lang

Advised and assisted Director of the largest US Army Printing and Publication Center in planning, organizing and coordinating the center's activities. Directed the daily operation of the military base. Advised Director on ADP security policy. Orchestrated actions within five divisions, ensuring customer requests were fulfilled in a timely manner. Prepared and coordinated internal/external actions and correspondence for Director. Developed and controlled the annual budget for the organization. Organized and chaired ADP Users Group, performed security needs analysis, designed computer security systems and evaluated security systems within the installation, to maximize protection of ADP assets and data. Project Manager to acquire over $1,000,000 new equipment. Deputy Installation Coordinator, developing and implementing policies/procedures for control, operation and maintenance of the military installation.

Employment Dates: 1974 - 1989
Company & Title: US Army
US Army, Chief Warrant Officer 4
Data Processing Technician / ADP Security Technician
Data Processing Systems Repair Technician
Command and Control Systems Test Officer

Positions of increasing scope and responsibility maintaining, operating, controlling and logistically supporting a variety of mainframe computers, minicomputers computers, electronic command control and communications systems, radar and identification friend or foe (IFF) equipment. Project Manager for the Operational Testing of equipment being considered for procurement by the US Army and other DOD agencies. Operations Officer of an organization responsible for performing COMPUSEC evaluations of top secret DOD, Dept. of Army and contractor computer facilities. Managed the daily operations and administrative functions of large organizations. Experience also included repairing and supervising repair of complex electronic equipment down to component level utilizing general and special purpose test equipment. Wrote, tested and implemented computer programs in support of logistics and financial tracking systems. Taught basic and advanced computer theory and troubleshooting at the US Army Air Defense School.

OTHER ACTIVITIES AND PROFESSIONAL AFFILIATIONS

- Member of the Technical Committee, Software Engineering Laboratory, Fraunhofer Center - Maryland,
- Member of the Steering Committee, Software Engineering Consortium - Maryland,
- Chairman of the Program Committee for the IT Sub-Committee for the High Technology Council of Maryland,
- Member of the Technical Committee for Practical Systems Measurement
- Member of the Program Managers Institute

OAO Corporation

7500 Greenway Center Drive • Greenbelt, Maryland 20770-3502
(301) 345-0750 • Fax: (301) 345-9669

September 29, 1999

Mr. Jeff Grove
Staff Director
Technical Subcommittee
Committee on Science
2319 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Grove:

Mr. Charles W. Talley, Director of OAO's Information Engineering Center (IEC) will testify before your committee, September 30, 1999 on the review of the Computer Security Enhancement Act of 1999. In his position as Director, IEC, Mr. Talley is responsible for managing software and systems development projects for numerous federal agencies. In the past two years Mr. Talley has been responsible for the following projects that have contained some element of computer security within the total task requirements:

1997:
Department of Transportation, US Coast Guard, Implementation of the Fleet Logistics System, $3.5M

1998:
Department of Transportation, US Coast Guard, Implementation of the Fleet Logistics System, $3.5M
US Air Force, Surgeon Generals Office, Medical Performance Measurement Task, $1.75M

1999:
Department of Transportation, US Coast Guard, Implementation of the Fleet Logistics System, $3.5M
US Air Force, Surgeon Generals Office, Medical Performance Measurement Task, $1.75M
Federal Aviation Administration, National Credit Card Implementation Program, $80,000
General Services Administration, Inventory Control Program, $150,000

This list is the total of the projects and monies received by OAO Corporation for projects that were managed by Mr. Talley and involved elements of computer security.

Sincerely,

Bruce U. Hair, Ph.D.
Vice President
Information Technology Division

Document No. 35