H.R. 285: DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY ENHANCEMENT ACT OF 2005

HEARING

BEFORE THE

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

APRIL 20, 2005

Serial No. 109–11

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE

22–904 PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania, *Vice Chairman*
CHRISTOPHER SHAYS, Connecticut
PETER T. KING, New York
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
JIM GIBBONS, Nevada
ROB SIMMONS, Connecticut
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
DAVE G. REICHERT, Washington
MICHAEL MCCAUL, Texas
CHARLIE DENT, Pennsylvania
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

SUBCOMMITTEE ON ECONOMIC SECURITY, INFRASTRUCTURE PROTECTION, AND CYBERSECURITY

DANIEL E. LUNGREN, California, *Chairman*

DON YOUNG, Alaska
LAMAR S. SMITH, Texas
JOHN LINDER, Georgia
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
MIKE ROGERS, Alabama
STEVAN PEARCE, New Mexico
KATHERINE HARRIS, Florida
BOBBY JINDAL, Louisiana
CHRISTOPHER COX, California *(Ex Officio)*
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
PETER A. DEFAZIO, Oregon
ZOE LOFGREN, California
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
JAMES R. LANGEVIN, Rhode Island
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

CONTENTS

Page

STATEMENTS

The Honorable Daniel E. Lungren, a Representative in Congress From the State of California, and Chairman Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity .....
The Honorable Loretta Sanchez, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity .....
The Honorable Christopher Cox, a Representative in Congress From the State of California, and Chairman, Committee on Homeland Security .....
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security
Oral Statement .....
Prepared Statement .....
The Honorable Bobby Jindal, a Representative in Congress From the State of Louisiana .....
The Honorable John Linder, a Representative in Congress From the State of Georgia .....
The Honorable Zoe Lofgren, a Representative in Congress From the State of California .....
The Honorable Stevan Pearce, a Representative in Congress From the State of New Mexico .....

WITNESSES

Ms. Catherine Allen, President and CEO, BITS, Financial Services Roundtable
Oral Statement .....
Prepared Statement .....
Mr. Paul Kurtz, Executive Director, Cyber Security Industry Alliance
Oral Statement .....
Prepared Statement .....
Mr. Harris Miller, President, Information Technology Association of America
Oral Statement .....
Prepared Statement .....
Mr. Ken Silva, Chairman of the Board of Directors, Internet Security Alliance
Oral Statement .....
Prepared Statement .....
Mr. Amit Yoran, President, Yoran Associates
Oral Statement .....
Prepared Statement .....

APPENDIX

Questions and Responses from Ms. Catherine A. Allen .....
Questions and Responses from Mr. Paul B. Kurtz .....
Questions and Responses from Mr. Ken Silva .....

H.R. 285: DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY ENHANCEMENT ACT OF 2005

Wednesday, April 20, 2005

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON ECONOMIC SECURITY,
INFRASTRUCTURE PROTECTION, AND CYBERSECURITY,
COMMITTEE ON HOMELAND SECURITY,
Washington, D.C.

The subcommittee met, pursuant to call, at 11:05 a.m., in Room 210, Cannon House Office Building, Hon. Dan Lungren [chairman of the subcommittee] presiding.

Present: Representatives Lungren, Souder, Pearce, Jindal, Cox (ex officio), Sanchez, Dicks, Lofgren, Langevin, Thompson (ex officio), and Linder.

Mr. LUNGREN. The Committee on Homeland Security Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity will come to order. The subcommittee is meeting today to hear testimony on H.R. 285, the Department of Homeland Security Cybersecurity Enhancement Act.

In 1983, the film "War Games" depicted smart, tech-savvy teenagers finding a back door into the Department of Defense tactical computer. Mistaking real life for a war game, they inadvertently bring the country to the brink of a nuclear war. Although enjoyable as a film and fictional, the movie is a stark reminder of the potential threats, vulnerabilities and consequences of cyberattack.

Today's world is even more interconnected through cyberspace, not just through the use of computers, but because of our increasing reliance on cybersystems to control our national infrastructures and economy.

Ensuring that essential services and industries survive an attack has always been a part of our national security strategy. What is new is how cyberspace networks have created complex interdependencies that have never existed to this extent before. The complexity and extent of these networks is not fully understood. The technology and networks are themselves constantly changing.

Identifying what is critical is becoming simultaneously more difficult and more vital. Furthermore, the majority of critical infrastructure is outside of Federal control, with 85 percent in private hands. The Department must work hand in hand with the private sector not only because the majority of structure is owned privately, but because the private sector is at the forefront of innova-

tive, productive and efficient technologies to secure cyberspace and associated critical infrastructure.

Many of us recognize the average cyberattack such as a worm or virus is a nuisance, one that irritates us, slows down our computers or prevents us from e-mailing. Yet deliberate cyberattacks have the potential to do physical harm in the form of attacks on cybersystems controlling critical infrastructures, such as dams and power plants or medical systems. Since I live just downriver of a dam, I am particularly acutely aware of that. They can also be launched coincident with physical attacks to interfere with our response and to make a bad situation even worse.

It is typical to measure the potential cost of probabilities of such attacks. There are no standard methodologies for cost measurement, although the 2003 loss estimates due to hostile digital acts range from $13 billion, worms and viruses only, to $226 billion for all forms of overt attacks.

Although accidental, the blackout of August 2003 may have cost us about 6—to $10 billion for the U.S. economy alone, which would amount to 1/10 of 1 percent of GDP. Clearly if the attack had been deliberate, the potential loss could have been much worse, and an attack on the financial services sector or the stock market could have incalculable long-term economic repercussions.

Recognizing this importance of cybersecurity to homeland and economic security, the Congress, when it created the Department of Homeland Security, directed this new department to lead the effort to develop a comprehensive cybersecurity strategy for the Nation. In response, the Department established the National Cybersecurity Division within the Information, Analysis and Infrastructure Protection Directorate headed by a Director reporting to the Assistant Secretary of Infrastructure Protection.

As chairman of the subcommittee, I appreciate the oversight work that was done by the Select Committee on the Homeland Security Subcommittee on Cybersecurity, Science, and Research and Development during the last Congress, which culminated in the subcommittee's excellent report entitled Cybersecurity for the Homeland.

The report makes clear that under current organizational structure, cybersecurity has not received the priority and attention it deserves within the Department, and that the National Cybersecurity Division needs explicit statutory duties and authorities. These findings led to the drafting and introduction of the bill that we are considering today, H.R. 285, the DHS Cybersecurity Enhancement Act of 2005, which was introduced earlier this year by Congressman Mac Thornberry, the former subcommittee chairman, and Congresswoman Zoe Lofgren, the former Ranking Member and currently a member of our subcommittee.

I am pleased we have an excellent panel of witnesses today to help the subcommittee examine the need for this legislation. In particular. We will hear from Mr. Amit Yoran, who was the first Director of the National Cybersecurity Division with DHS, and is a highly regarded cybersecurity expert. He left the Department after 1 year and is in the unique position to help us explore the challenges of cybersecurity within DHS.

Passage of H.R. 285 would not solve all of the problems with cybersecurity within DHS, but it would elevate the mission within the Department by creating a new position of Assistant Secretary of Cybersecurity. This change would give the head of the National Cybersecurity Division not only increased prominence within the Department, but also give this official greater clout across the Federal Government and the private sector.

The bill also contains specific language that would outline the responsibilities of the assistant secretary, guiding the work that needs to be done to identify the threats and vulnerabilities, mitigate those vulnerabilities, institute a warning system, and be able to effectively and quickly respond to an attack should one occur.

These statutory authorities will also serve to clarify within DHS for the outside world the role and responsibilities of the DHS Cybersecurity Office. Under the bill, the assistant secretary also would assume authority over the National Communications System, which will bring an end to DHS's current treatment of telecommunications as separate from information technology. This is essential because the real world convergence of telephony and data is proceeding rapidly, and DHS must integrate policy for securing these elements of the cyberworld.

Today we have witnesses who represent the leading experts in the cybersecurity industry with extensive experience working either in or with DHS. We look forward to hearing from them and why they think this legislation is important, presuming they do believe it is important.

I would thank you all for appearing today.

I would recognize the Ranking Member Ms. Sanchez for any opening remarks you would make.

Ms. SANCHEZ. Thank you, Mr. Chairman, and thank you all for appearing before us today. We are looking forward to your testimony. This morning we are going to hear testimony, and this afternoon we are going to mark up H.R. 285, the Department of Homeland Security Cybersecurity Enhancement Act of 2005.

I am so proud that this was written by my good friend from California Ms. Zoe Lofgren and by Mr. Thornberry of Texas in the last Congress when they had the roles of heading up the subcommittee that handled cybersecurity, which of course now has been put into this larger committee. I congratulate both of them for the diligent work that they did and for bringing it forward.

I am very grateful to the chairman of this committee and to Mr. Cox and our Ranking Member Bennie Thompson for seeing the necessity to bring this forward early in this session so that we could get it done.

I know that it is a very bipartisan manner in which Ms. Lofgren and Mr. Thornberry worked on this. I am happy to be a cosponsor of this particular bill. I think it is incredibly important that we look at the cybersecurity component of our economic security of this country, in particular banking and finance. I myself used to work in that arena on Wall Street. I believe it is just incredibly important for us to make sure that we do secure this.

I hope that this bill, H.R. 285, will raise the visibility of the need to really explore cybersecurity, understand it, and get that under control so that we don't have an attack on either one of our infra-

structure pieces, like a dam, for example, or, more importantly, that we don't lose everybody's money somewhere out in cyberspace or to the bad guys.

So I am looking forward to this. I think having an assistant secretary is going to be important, and that person will be able to raise the visibility of this. I am confident that we are going to pass this piece of legislation.

So, thank you, Mr. Chairman, and I—.

Ms. LOFGREN. Would the gentlelady yield?

Ms. SANCHEZ. Should I yield to her, or will you be recognizing her?

Mr. LUNGREN. I was going to recognize her after I recognize the chairman of the full committee.

Ms. LOFGREN. Okay.

Mr. LUNGREN. The chairman of the full committee.

Mr. COX. Thank you very much.

Since we are about to hear from Congresswoman Lofgren, and since Mr. Thornberry is not here, let me acknowledge both of them, and thank you for your leadership on this legislation. The Homeland Security Committee has organized itself again, as we did as a select committee in the preceding Congress, in subcommittee around this mission of cybersecurity. It is the fact that not only is the Department of Homeland Security, our newest Cabinet department, already the third largest Cabinet department, but, in addition, it is the locus within the Federal Government for a new mission not just for our government, but for our country, and that is cybersecurity.

It is the focal point within the Federal Government for all of our efforts not just at the government level, but also internationally and in the private sector, to prevent harm to our national security and to our economy from cyberattacks.

We have, I think, some skeletal frameworks from which to work: HSPD 7, the President's National Strategy to Secure Cyberspace, the National Response Plan to the extent that it treats cyberincidents. But what we need clearly inside the Department of Homeland Security is leadership, and that entails organizational responsibility and the opportunity to lead. So this Committee in the 109th Congress, the Select Committee in the 108th, have identified, with our partners outside the government, this organizational step as a key one, the step that we are proposing to take in this legislation.

I am very, very anxious to hear from our witnesses today to make sure that we continue on the right track. But I believe that an extraordinary amount of thought has been given to this over the period of now a few years under the leadership of Mr. Thornberry and Ms. Lofgren. So I want to thank you for that leadership.

I want to thank the chairman and Ranking Member of this subcommittee for renewing our efforts as a Homeland Security Committee and to see this job through completion. I hope that today's hearing moves us along on that path.

Mr. LUNGREN. Thank you, Mr. Chairman.

Before we hear from the panel, I would recognize the gentlelady from California Ms. Lofgren, who is the author of the bill and a member of this subcommittee.

Ms. LOFGREN. Thank you very much, Mr. Chairman.

I do believe this bill is very important, and as has been mentioned, it is very bipartisan in nature. It was largely prepared through the direction of Congressman Mac Thornberry and myself in our roles in the last Congress in the Cybersecurity Subcommittee. Want to thank Mac Thornberry and also his staff for their collaboration and hard work on this bill. I am really very proud of the work that Mac and I did in a truly bipartisan way on the issue of cybersecurity in the last Congress.

During that 108th Congress, the subcommittee conducted many hearings and briefings from Members of Congress and staff on cybersecurity issues. The subcommittee also reached out to diverse groups of individuals on seeking ways to improve cybersecurity for the Nation. Since May of 2003, 15 hearings and briefings were conducted, as well as additional and formal meetings with Members and staff. We heard from private sector experts who operate critical information infrastructure; Federal, State and local officials; academic experts and the like. A variety of witnesses also discussed the Department of Homeland Security's role and responsibilities in securing cyberspace.

To make a long story short, as the chairman of the full committee has mentioned, we do have an adopted strategy, but the strategy has not yet been implemented. It has become clear to myself and Congressman Thornberry and many, many others that we need a higher level of attention within the Department. Obviously, there is much to do. This bill will not in and of itself solve the issues, but it will put us on a footing, we believe, to actually get the attention that we need.

The position would be an Assistant Secretary of Cybersecurity within the Information, Assurance and Infrastructure Protection Directorate, and the second—the path the bill also accomplishes is to define cybersecurity at the department level so that a consistent and authoritative definition can be integrated throughout the Department.

I would ask that my full statement be submitted for the record, but I would note that the Department of Homeland Security is not alone in focusing on the issue of cybersecurity. Clearly most of the infrastructure is within the private sector, not within the government. NSF has recently engaged in a very important funding of research in the cybersecurity area with a number of academic institutions. One of them, Professor Shankar Sastry at the University of California, who has been very helpful to us on this effort, was recently quoted and talking about the issue of cybersecurity, that we don't want to have a digital equivalent of Pearl Harbor.

So right now we are worried about viruses and worms, but the exposure that we have is very large. We are very behind in where we need to be to protect the infrastructure of the Nation. So this is serious stuff. I believe that adopting this bill promptly will get us further down the road to where we need to be.

I appreciate the support of the chairman and Ranking Member, both of the full committee and the subcommittee, in promptly moving this forward.

I yield back the balance of my time, and I thank you.

PREPARED STATEMENT OF THE CONGRESSWOMAN ZOE LOFGREN

• This bill addresses an issue that I believe is very important making sure that our government, working together with the private sector and academia, is doing all that it can to ensure that cyber security is a top priority in our nation's homeland security strategy.

• This bill is bipartisan in nature and was largely prepared through the direction of Representative Mac Thornberry and myself in our roles as leaders of the Cyber security Subcommittee last year. I thank Mac and his staff for their collaboration and hard work on this bill, I am proud to have been able to work with him in a truly bipartisan fashion to address this great need.

• During the 108th Congress, the Subcommittee conducted numerous hearings and briefings fro Members of Congress and staff on cyber security issues. The Subcommittee also reached out to diverse groups and individuals on ways to improve cyber security for the nation. Since May 2003, fifteen hearings and briefings were conducted, as well as several other informal sessions with Members and staff. The committee heard from private sector experts who own and operate critical information infrastructure. Federal, state and local government officials and academic experts testified on the need to fortify the nation's cyber security. A variety of witnesses also discussed the Department of Homeland Security's role and responsibilities in securing cyberspace.

• The subcommittee initially focused its oversight on the key management functions required for the success of any organization. Through hearings and oversight letters, the Subcommittee questioned DHS about its cyber security mission and functions. The subcommittee was also interested in how DHS was developing working definitions related to cyber security and what progress it was making to implement a viable organizational structure, as well as formal personnel, resource and programmatic efforts.

• Unfortunately, the level and detail of planning documents needed to manage the new cyber mission within DHS was not forthcoming. Budget paperwork throughout the fiscal year was vague. It is still unknown whether spending plans and detailed budget execution data exists.

• These are some of the reasons why I believe this bill is necessary and can only help to improve our nation's level of cyber security.

• This bill accomplishes two essential tasks: it establishes an Assistant Secretary of Cyber Security within the Information Assurance and Infrastructure Protection Directorate to prioritize cyber security and protect our computer networks.

• The position, at this higher level, will be better able to coordinate with other Assistant Secretaries within the Directorate, as well as officials throughout the Department, other federal agencies, and the private sector.

• The second task this bill accomplishes is to define cyber security at the Department level, so that a consistent and authoritative definition can be integrated throughout the Department's mission and policy functions.

• I continue to hear from cyber security experts about the threats and vulnerabilities facing our nation's networks and systems.Unfortunately, these continue to grow faster than our nation can address them.

• These vulnerabilities will continue to hamper our homeland security efforts if we do not make cyber security a major priority.As long as our critical infrastructures are interconnected and interdependent, the likelihood that a cyber attack will disrupt major services or cripple our economy will remain and the threat will increase.

• If a cyber attack occurred simultaneously as a physical attack, critical emergency response systems and communications operations could be taken out, increasing the casualties and confusion of an attack.

• The Department needs to be advancing on cyber security - it cannot afford to sit back and make minimal, if any, progress in this area. It certainly needs to be doing more than re-creating programs that existed before the Department's creation.Unfortunately, that is all that is happening today.

• I fear that the Department is unable to move forward on cyber security because it lacks the leadership necessary to focus on its unique and cross-cutting nature. The individual responsible for leading the government's cyber security efforts must have more authority within the Department of Homeland Security.

• I recognize that the government cannot develop plans for physical security in a vacuum—those dealing with both of those issues must be able to communicate and collaborate. At the same time, though, the government cannot be naïve in its approach. The first responders and security actors for cyber assets are not the same as in the physical world. This bill recognizes this difference, while keeping in place the mechanisms for collaboration with the Infrastructure Protection Directorate.

• Thank you Chairman Cox and Ranking Member Thompson for bringing this bill before us today. I am certain that our discussion that we are about to have on the merits and the importance of this bill.
• I know that some may argue that this bill is unnecessary and that the Department already has authority to do this work now. If that is true, then I ask why it has not been done already. In our role of as the authorizers and the overseers of the Department of Homeland Security, I believe it is critical for us to give the Department guidance as to how it should manage the tremendous tasks that it has been given. To sit by and do nothing would place our nation in greater danger than it is today, and I for one am unwilling to do nothing.
• I strongly urge you to vote in favor of this bill.

Mr. LUNGREN. I thank the gentlelady for her comments and congratulate her on this piece of legislation.

Other members of the committee are reminded that opening statements may be submitted for the record.

We are pleased to have the distinguished panel of witnesses before us on this important topic.

The Chair now recognizes Mr. Amit Yoran, the president of Yoran Associates and the former Director of the National Cybersecurity Division of the Department of Homeland Security.

Before you testify, could you tell me if I am pronouncing your name correctly?

Mr. YORAN. Yes, sir, that was perfect.

Mr. LUNGREN. Very good. Thank you.

All witnesses should know that your written testimony will be submitted for the record. I would ask that you try to limit your comments to 5 minutes so that we can make sure that we hear all of you and then get involved in Q and A.

Mr. Yoran.

STATEMENT OF AMIT YORAN, PRESIDENT, YORAN ASSOCIATES

Mr. YORAN. Good afternoon, Chairman Lungren and distinguished members of the subcommittee. I would like to first thank Congressman Thornberry and Congresswoman Lofgren and their staffs for their tireless efforts in the important topic of cybersecurity and for the entire subcommittee's bipartisan attention to this important topic.

My name is Amit Yoran, and I am pleased to have the opportunity to appear before the subcommittee today to discuss enhancements to our national efforts to secure cyberspace. I am president of Yoran Associates, a technology strategy and risk advisory business headquartered in northern Virginia.

In our practice we advise a number of global enterprises on their technology strategy and mitigating associated business risks and exposures. Prior to founding Yoran Associates, I served as the Director of the National Cybersecurity Division of the Department of Homeland Security responsible for building a national cyberresponse system, a national threat and vulnerability reduction program, a national cyberawareness and training program, and establishing increased security and coordination among and between government and international counterparts. Much work has been done in the implementation of the above responsibilities by both the public and private sectors, and even more work remains ahead of us.

Protecting America from physical threats is a concept well understood by senior leadership and risk managers, where sound understanding of the challenges, consequences of failure and specific work plans to be accomplished are ongoing as part of a unified protection effort. Our ability to conceptualize and defend against physical threats has matured over many years. Changes to critical infrastructures do not occur on a highly dynamic basis.

On the other hand, our use of and reliance on technology transforms continually in today's modern competitive environments. Significant challenges remain in raising awareness and understanding of vulnerabilities to cyberfailure or attacks to the leadership which structure and resource defensive efforts. The challenge to change our thinking is consistent in both the government and private sector.

Since the creation of the Department of Homeland Security approximately 2 years ago, a massive restructuring has occurred in the Federal Government. More important than the restructuring and the organizational charts is the fantastic work being accomplished by so many talented and dedicated public servants serving in the most noble and challenging of undertakings, protecting our homeland and the American people.

Responsibility for protecting these business-critical systems lies largely in the private sector, where nearly all of these critical infrastructure systems are owned and operated. Organizational leadership must encourage the inclusion of technology risks into their business risk management practices. Responsible business risk practices require a thorough evaluation and informed acceptance of technology and business exposures, or investment in risk mitigation techniques. Forward-thinking organizations are protecting themselves from significant threats and exercising their response plans in simulated cybercrisis scenarios. These types of activities can be used effectively to create awareness among organizational leadership. In essence, industry must not wait for government action before securing systems and improving their organizational policies and procedures.

Some critical functions and responsibilities in our national cybersecurity efforts are inherently governmental, such as providing a survivable communications capability in various bad-case cyber and telecommunications outage scenarios, raising the awareness of threat information and coordinating national response efforts. I challenge the committee to assist the Department in increasing the investments being made in fundamental cybersecurity research and development.

Secretary Chertoff is in the midst of his departmental analysis and restructuring effort, the second stage review. The Directorate of Information Analysis and Infrastructure Protection under which the National Cybersecurity Division resides is charged with performing some of the most important mission functions of DHS. It is imperative that we afford the Secretary the opportunity to design and structure the Department to the best of his ability and satisfaction and to provide him and his team whatever support we can in accomplishing their mission. Creating greater unity and clarity around cyberefforts will result in further inclusion and better integration of cybersecurity thinking, awareness and protective

measures across all of the various programs and efforts taking place to protect America.

The creation of an assistant secretary position to address cybersecurity issues is not inconsistent with a unified or integrated risk management approach. On its own, it does not address the government's challenges in cybersecurity. There are several areas where greater clarity is needed and support must be given to centralize cybersecurity functions across the government. The Department of Homeland Security struggles with its mission responsibility of security for government computer systems, but FISMA authorities lay entirely within OMB. Consideration of this topic by the committee can provide needed attention and have significant impact on improving operations on government cyberpreparedness.

Procurement practices by the Federal Government to enhance cybersecurity features, functionality and requirements are not effective and are rarely enforced with consistency, resulting in the single greatest missed opportunity to positively influence and drive better security capabilities into the products that are used by both government and private sectors.

There are many dedicated Americans in both the public and private sector working on these challenges to our economic and homeland security. It is my hope that the Committee on Homeland Security can provide them further mission guidance, support our common cause and assistance wherever possible.

I look forward to answering any questions you may have.

Mr. LUNGREN. Thank you very much, Mr. Yoran.

[The statement of Mr. Yoran follows:]

PREPARED STATEMENT OF AMIT YORAN

Good afternoon, Chairman Lungren and distinguished Members of the Subcommittee. My name is Amit Yoran and I am pleased to have an opportunity to appear before the subcommittee today to discuss enhancements to our national efforts to security cyberspace. I am the President of Yoran Associates, a technology strategy and risk advisory business headquartered in Northern Virginia. In our practice, we advise a number of global enterprises on their technology strategy and associated business risks and exposures. Prior to founding Yoran Associates I served as the Director of the National Cyber Security Division of the Department of Homeland Security (DHS), responsible for building, (1) a national cyber response system; (2) a national threat and vulnerability reduction program; (3) a national cyber awareness and training program; and (4) establishing increased security and coordination among and between government and international counterparts. Much work has been done in the implementation of the above responsibilities by both the public and private sector and even more work remains ahead of us.

Protecting America from physical threats is a concept well understood by senior leadership and risk managers, where sound understanding of the challenges, consequences of failure, and specific work plans to be accomplished are ongoing as part of a unified protection effort. Our ability to conceptualize and defend against physical threats has matured over many years. Changes to critical infrastructures do not occur on a highly dynamic basis. On the other hand, our use of and reliance on technology transforms continually in modern competitive environments . Significant challenges remain in raising awareness and understanding of vulnerability to cyber failures or attacks to the leadership which structure and resource defensive efforts. This challenge to change our thinking is consistent in government and the private sector.

Since the creation of the Department of Homeland Security, approximately two years ago, a massive restructuring has occurred in the Federal Government. But more important than the restructuring and the organizational charts is the fantastic work being accomplished by so many talented and dedicated public servants serving in the most noble and challenging undertakings; protecting our homeland and the American people.

The task in securing America's cyber infrastructures is a daunting and very real challenge. Efforts to secure the computer systems on which our nation's critical infrastructures and our economic stability rely are being addressed with a pre-9/11 lack of urgency. As we failed to grasp the gravity of the World Trade Center bombings in 1993, today we are not acting aggressively on the numerous warning signs of critical infrastructure computer failures; the Northeast-Midwest blackout of 2003, ATM outages and airline system failures or on the numerous computer threats actively working against our economic security. Simply put, many American business interest have a significant if not complete reliance on general purpose computers and inter-connected networks which can generally be categorized as untrustworthy. The recipes for disaster are present.

Responsibility for protecting these business critical systems lies largely in the private sector where nearly all of these critical infrastructure systems are owned and operated. Organizational leadership must encourage the inclusion of technology risks into their business risk management practices. Responsible business risk practices require a thorough evaluation and informed acceptance of technology and business exposures or investment in risk mitigation techniques. Forward thinking organizations are protecting themselves from significant threats and exercising their response plans in simulated cyber crisis scenarios. These types of activities can be used to effectively create awareness among organizational leadership. In essence, industry must not wait for government action to begin securing systems and improving organizational policies and procedures.

Some critical functions and responsibilities in our national cyber security efforts are inherently governmental, such as providing a survivable communications capabilities in various bad-case cyber and telecommunications outage scenarios, raising awareness of threat information and coordinating national response efforts. I challenge the Committee to assist the Department in increasing the investments being in fundamental cyber security research and development.

Secretary Chertoff is in the midst of his departmental analysis and restructuring effort—the second stage review. The Directorate of Information Analysis and Infrastructure Protection under which the National Cyber Security Division resides, is charged with performing some of the most important mission functions of DHS. It is imperative that we afford the Secretary the opportunity to design and structure the Department to the best of his ability and satisfaction and to provide him and his team whatever support we can in accomplishing their mission. Creating greater

unity and clarity around cyber efforts will result in the further inclusion and better integration of cyber security thinking, awareness and protective measures across all of the various programs and efforts taking place to protect America.

The creation of an Assistant Secretary position to address cybersecurity issues is not inconsistent with a unified or integrated risk management approach. On its own it does not address the Government's challenges in cyber security. There are several areas where greater clarity is needed and support must be given to centralize cyber security functions across government. The Department of Homeland Security struggles with its mission responsibilities of security for government computer systems, but FISMA authorities lay entirely within OMB. Consideration of this topic by the Committee can provide needed attention and have significant impact on improving operations and government cyber preparedness. Procurement practices by the Federal Government to enhance cyber security features, functionality and requirements are not effective and are rarely enforced with consistency, resulting in the single greatest missed opportunity to positively influence and drive better security capabilities into the product sets used by both government and private sectors.

There are many dedicated Americans in both the public and private sector working on these challenges our economic and homeland security. It is my hope that this Committee on Homeland Security can provide them further mission guidance, support our common cause and assistance wherever possible. I look forward to answering any questions you may have.

Mr. LUNGREN. The Chair now recognizes Mr. Harris Miller, president of the Information Technology Association of America, to testify. I must say I knew Mr. Miller in another life when he was neither as well dressed or as profitable-looking as he is now. It is good to see you have reached success in your older years.

STATEMENT OF HARRIS N. MILLER, PRESIDENT, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA

Mr. MILLER. Thank you, Mr. Chairman. It is a great honor and pleasure to be here in front of Lungren 2, Congressman Lungren's return. We got the great opportunity to work with you on the Judiciary Committee. It was a great honor and pleasure to serve you there. It is a great honor to appear before you, Congresswoman Sanchez, Chairman Cox and Ranking Member Thompson, and other members of the subcommittee today.

I want to join in commending Congressman Thornberry and Congresswoman Lofgren for introducing this important legislation, and I urge the subcommittee to pass it and move it through the full committee of the House, and we hope to get cooperation from the other side of the Hill, too.

Exhibit A about why this legislation is sitting immediately to my right. Mr. Yoran is too much of a gentleman to perhaps explain fully why he is back in the private sector after a relatively short period of time in the government, and I am not going to put any words in his mouth, but we at the private sector were very excited when he agreed to come back into government to serve in this position.

But we felt that because of where the position is located in the Department, a head of a division as opposed to an assistant secretary level, that a lot of the ideas and work and enthusiasm that might have been brought to the position simply couldn't be done because of where the position is located.

We also commend the current Acting Director Mr. Purdy. He is also trying very hard. But at the end of the day, Mr. Chairman, as you know very well, in this town where you stand is where you sit; and where you sit is where you stand. When you are down as a head of a division, you simply cannot bring the firepower and the

leadership to the issue that you can as an assistant secretary, a confirmable position.

So we think that the idea that Congressman Thornberry and Congresswoman Lofgren have incorporated into this legislation is critical. We urge you and the subcommittee to move it forward.

Certainly, a couple of simple points, number one, prior to the formation of the Department of Homeland Security, the cybersecurity issue was so important in this administration that the position was a special advisor to the President of the United States. That is where the locus of this government's focus on cybersecurity was. After the Department was formed, it was—ended up—as a head stuck in a division. That shows you that without any real indication of any change of the importance of the issue in terms of our country and protecting our homeland, the position was significantly downgraded. As a result, a lot of the work that President Bush and his administration put into the National Strategy to Secure Cyberspace, which was released a little over 2 years ago, frankly hasn't been implemented because we have not had the type of leadership we need. This is no slap on Secretary Ridge and now Secretary Chertoff, but at the end of the day, if you don't have someone high enough in the organization to show leadership on the issue, it simply isn't going to happen.

Now we understand that—the argument on the other side, that physical security and cybersecurity need to be closely integrated. That is why they initially didn't want to have an Assistant Secretary for Cybersecurity because it not was not thought to be a separate issue. We understand that there is an argument on that side, But we happen to think it is inaccurate for reasons that Mr. Yoran indicated.

Just think about it. At the end of the day, people are much more afraid of bombs and anthrax than they are of viruses and worms. They have a lot of experience of dealing with these physical threats. But the cyberworld is much different. It is much more out there in cyberspace, so to speak, and people don't quite understand it. So, again, putting it in the physical arena, the resources, the attention, the expertise and the government was all loaded toward people on the physical side, which is incredibly important, Mr. Chairman. We are not saying it is not, but it simply is different.

There is also a fundamental cultural issue. How many people involved in law enforcement and physical threats have ever gone to cyberschool, and how many cybergeeks have ever gone to physical school? They simply live in different cultures, in difference worlds. Now there are a few people that have skills on both sides, but it is a different world. It is a different set of issues.

Again, having someone in government who understands that fundamentally at the right level of government, at the assistant secretary level, we think is critically important to furthering the agenda that is absolutely necessary. It is all about resource allocation. It is all about allocating those resources, and it is all about having the ear of the people at the top.

At the end of the day, Mr. Chairman, as you said in your opening statement, 85 percent of our critical infrastructure is controlled by the private sector. One of the most important roles the government can play in cybersecurity is as a bully pulpit, getting out in front

of people in the private sector to explain to them why they have to put as much priority on cybersecurity as they do on physical security, why they can't always be trying to turn around and say, what is the ROI on this? Again, I ask you, is it more likely to be successful if that person sending that message is an Assistant Secretary for Cybersecurity, or is it someone who frankly is pretty far down in the bureaucracy?

Mr. Chairman, as you said your opening statement, creating an assistant secretary is not going to solve all the problems, but it will get the cybersecurity issue back to the level of attention it had prior to the creation of the Department of Homeland Security. It will enable us to move forward with so many great ideas, which are included in President Bush's National Strategy.

I think moving this legislation will be very important to the protection of our Nation's homeland.

Mr. LUNGREN. Thank you, Mr. Miller.

[The statement of Mr. Miller follows:]

PREPARED STATEMENT OF HARRIS N. MILLER

Introduction

I am Harris N. Miller, President of the Information Technology Association of America (ITAA), representing over 380 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 software, services, systems integration, telecommunications, Internet, and computer consulting fields. These firms are listed on the ITAA website at *www.itaa.org*.

I appreciate this Subcommittee taking time from its very busy schedule to hold this hearing today on the need to elevate the issue of cyber security within the Department of Homeland Security (DHS) by creating an Assistant Secretary for Cyber Security. The constant attention by this Committee to the importance of cyber security in protecting our nation against terrorism is greatly appreciated by my members and all IT customers, whether they be individuals or companies.

After a lull in major network exploits, we have seen the issues of information security and critical infrastructure protection spring back into the news with the recent data breaches experienced by data brokers, database companies, universities, payroll processors and other types of organizations. As the development and adoption of electronic commerce evolves, 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 electronic commerce and the growth of the U.S. economy.

ITAA has played a major role in addressing the numerous issues of enhanced information security and cyber crime prevention. Our information security program dates back to 1999, with active participation from 250 IT companies. Since that time, along with many other accomplishments, ITAA has been proud to serve as a co-founder of the National Cyber Security Partnership, to chair the Partnership for Critical Infrastructure Protection, to co-found the National Cyber Security Alliance and the IT Information Sharing and Analysis Center (IT–ISAC) and to act as Sector Coordinator for the IT industry under Homeland Security Presidential Directive 7.

Why the U.S. Needs an Assistant Secretary for Cyber Security

Since the creation of the Department of Homeland Security, the Congress has become increasingly aware of the enormously complex challenges related to cyber security. The result is overwhelming bipartisan support in the committees of jurisdiction for a robust National Cyber Security Division (NCSD) to meet the broad challenges posed in the 2003 President's National Strategy to Secure Cyberspace. These challenges include creating and managing: a national cyber response system; a national program to reduce cyber security threats and vulnerabilities; a national cyber awareness and training program; and programs of coordination among federal, state and local governments, as well as with the private sector and with international partners.

ITAA, too, has been for several years advocating the need for a senior cyber security executive within the Federal government to help coordinate national cyber security policy among all industry, government and private sector stakeholders. We were the first organization to call for the creation of a cyber security "czar," and were very pleased that first President Clinton, by holding a White House meeting on cyber security in early 2000, and then President Bush, by establishing a cyber security advisor in the White House at the beginning of his term, each showed great leadership. But since the creation of the Department of Homeland Security, and the effective organizational demotion of the cyber security position, our concerns about Executive Branch leadership have returned.

Given strong bipartisan calls within Congress for a more robust NCSD capable of pulling together and coordinating among diverse entities within both government and the private sector, we feel very strongly that an Assistant Secretary position leading the NCSD is needed to meet the growing public administration, resource and policy challenges related to cyber security. This means coordinating closely with, but outside of, the Infrastructure Protection Division. When DHS was created, the decision was made to subsume cyber security coordination and outreach functions under an Assistant Secretary for Infrastructure Protection, on the premise that the integration of physical security and cyber security is better managed by one person, and that cyber security is only one component of physical security.

Our view, on the contrary, is that integration is best managed by two individuals, each experts in their respective fields, with a commitment to coordinating physical and cyber security where they are interrelated, with neither vital function subordinated to the other. It is clear that all of the nation's critical infrastructures, including water, chemicals, transportation, energy, financial services, health care, and others, rely significantly on computer networks to deliver the services that maintain our safety and national economy. It, therefore, is incumbent on the owners and operators of those critical infrastructures to manage improvements in the security of their information systems and to have a senior individual within the government, with effective influence and budget authority, who can coordinate collaborative efforts across critical infrastructure sectors and with state and local governments.

The NCSD has indeed made some progress; we applaud the valiant efforts of the former director and the current acting director and their creative and dedicated staff. But the current integration of cyber security and physical security is not working. As the IT Sector Coordinator, co-founder of the National Cyber Security Partnership and Chair of the Partnership for Critical Infrastructure Security—the cross-sectoral council of Federally-designated sector coordinators—ITAA has witnessed the growing demands the Congress has placed on the NCSD to implement policies consistent with and beyond the President's National Strategy to Secure Cyberspace. ITAA also has experienced ongoing frustration with the confusion in the NCSD and its unrealized potential.

Indeed, the President's National Strategy is not being implemented as quickly and fully as it should, in large part, we believe, because the current organizational structure at DHS allows cyber security priorities to be marginalized against other physical security activities considered to have higher priority. Good management is always about allocating resources to the highest priorities set by both the Department and Congress, but too often the cyber security function has suffered from missteps, and an increasing inability to meet the growing challenges that have been identified by Congress, government entities and the private sector.

Among them:

- DHS took several months to provide formal response to major private sector recommendations emerging from the December 2003 National Cyber Security Summit (see *www.cyberpartnership.org*), conducted in partnership with DHS and Secretary Ridge and designed to act on the President's National Strategy;
- A major "Partner Program" conference scheduled last year with industry and DHS was abruptly cancelled days before the event without explanation;
- The development of implementing regulations under the Homeland Security Act to protect critical infrastructure information (PCII) voluntarily submitted by private sector entities fails to facilitate information flows—as the law intended—from the private sector custodians of cyber security early warning, analysis, and forensics—to DHS. The IT–ISAC, for example, has submitted no critical cyber security information to DHS under this program, because the prescribed process does not reflect the realities of information management and proprietary business information within the private sector;
- DHS attempts to reorganize the private-sector "Sector Coordinator" and ISAC structures under Homeland Security Presidential Directive 7 proceeded against the counsel of several critical infrastructure representatives whose views may

have been better reflected in this DHS initiative had they been heard at a more senior political level—such as an Assistant Secretary—with guiding authority over staff;

• NCSD's cyber security R&D budget authority remains low and ineffectual. A division with an Assistant Secretary at the helm would likely command more resources; and

• It will not be until November of 2005 before we have a full cyber threat and attack exercise as a component of the DHS/industry critical infrastructure protection/emergency response exercises in the TOPOFF series, despite the real and identified threat of a coordinated physical/cyber attack on one or more of our critical infrastructures

The resulting bipartisan proposal within the Intelligence Reform bill to authorize the creation of an Assistant Secretary for Cyber Security underscores Congressional demands for a *confirmable* position of increased leadership within DHS that reflects the need for greater accountability to Congress.

Congressional Leadership

Last year, an amendment in the 9/11 bill creating the Assistant Secretary position was removed because of confusion during 11th hour negotiations. What was clear, however, was a White House position of "no objection" to the bill. Administrations as a matter of principle object to Congressional micromanagement of the President's organizational prerogatives. The official White House position of neutrality in this particular case, however, speaks volumes, in our view, about the level of support within the White House for an improvement in the functioning of the cyber security activities of DHS.

The House Subcommittee on Cyber Security, Science and Research & Development underscored the need for an Assistant Secretary in its December 2004 Report on Cyber Security for the Homeland. The Subcommittee cited creation of this position as one of six "core" areas in its cyber security roadmap for the future.

We wholeheartedly applaud and support Congress in its efforts to provide the legislative impetus for this important position, and accordingly support H.R. 285.

While we believe the Assistant Secretary position is critical, it is not the only critical step remaining in this journey. The cyber security threat is constantly changing, and Congress has a role in assuring that adequate investment is made in safeguarding critical infrastructure and the U.S. economy from next generation threats.

Practical steps involve increasing appropriations for cyber security research as authorized in the Cyber Security Research and Development Act of 2002. More research is needed to improve information systems, and identify and reduce their vulnerabilities. Congress should also authorize and appropriate increases in the funding of NIST to support its Computer Security Division—a critical resource in the development of computer security standards and best practices for the private sector and government agencies.

Congress should also act to encourage the private sector to adopt more rigorous information security practices. For instance, lawmakers should explore whether, and under what circumstances, commercially viable information security insurance can be used as a market driver toward improvements in information security management in the enterprise. Other potentially productive strategies include considering limits on liability from cyber security breaches for companies that implement industry-agreed practices and creating economic incentives for information security technology procurement and implementation

Finally, the Senate should ratify the Council of Europe Convention on Cyber Crime, signed by the United States in November 2001.

Conclusions

No government executive will create single-handedly the policies or regulations to herald a new age of information security or to make cyber vulnerability a thing of the past. Logic tells us that we have turned a corner in our reliance on the Internet, and that along with the many blessings of the information economy and the knowledge society come the risks posed by the cyber delinquent, cyber criminal and cyber terrorist. A responsible government takes the steps necessary to maximize the benefits and to manage the risks appropriately.

Creating an Assistant Secretary for Cyber Security advances the cause of information security, introducing practical advantages and sending an important symbolic message. Much needs to be done to improve the performance and to elevate the position of cyber security as an issue in the Administration, to coordinate information security across disparate government agencies, and to build the necessary bridges between the federal government and critical infrastructure industries. For far too long, the federal government's symbolic role in information security has gone begging—the "bully pulpit" stands empty. Consumers, small businesses and other orga-

nizations peg their response to various issues by the actions (or lack thereof) of policymakers. We believe that cyber security is one such issue.

In calling for the increased leadership that we believe an Assistant Secretary will bring to the goal of heightened cyber security, industry also stands ready to do its part—and the good news is that we have done much already. An ITAA-commissioned survey conducted by the University of Southern California's Institute for Critical Information Infrastructure Protection (ICIIP) at the Marshall School of Business identified 175 examples of cyber security enhancing products, services or activities from 65 responding organizations, including cross-sectoral and vertical industry groups and trade associations, multinational and owner-operated businesses, academic institutions, and professional societies. Intrusion detection and early warning networks, structures for information sharing, enhanced commercial products across an array of information security functionalities, guides, white papers, no-charge anti-virus protections and automatic software update capabilities are just some examples of the industry-led strides to raise the nation's cyber security profile.

The federal government faces a full agenda of cyber security issues. The challenges of providing critical infrastructure protection are formidable today and are likely to be even significant in the future. An Assistant Secretary for Cyber Security can make an important difference. We thank the Subcommittee for bringing this important issue to the attention of the American people.

Thank you very much.

Mr. LUNGREN. The Chair will now recognize Mr. Paul Kurtz, the executive director of the Cybersecurity Industry Alliance, to testify.

STATEMENT OF PAUL KURTZ, EXECUTIVE DIRECTOR, CYBER SECURITY INDUSTRY ALLIANCE

Mr. KURTZ. Thank you, Mr. Chairman. Thank you, Ranking Member Sanchez.

I want to recognize, as Amit and Harris have done, the work of Congressman Thornberry and Congresswoman Lofgren in putting together this piece of legislation. As executive director of CSIA, I am also pleased to speak on behalf of the Business Software Alliance on the need for an Assistant Secretary for Cybersecurity at DHS.

We want to urge early and urgent passage of H.R. 285. Since the late 1990s, we have spoken of a partnership to secure the critical infrastructure. For this partnership to work and to truly be successful and not be simply rhetoric, we need a clear leader in the Department of Homeland Security to act as the focal point.

A director or a deputy-assistant-secretary-level position does not have the sufficient stature, programmatic authority or accountability to reach across government and industry sectors. A leader in securing the critical infrastructure must have the authority and resources to accomplish this important and complex mission. This leader must be at least at the assistant secretary level to have the impact needed.

Unlike other sectors, the information infrastructure is dynamic. It will continue to evolve for the foreseeable future. Changes within the information infrastructure are driving change in all other sectors. Cyber and physical infrastructure security will receive greater respect and attention with an Assistant Secretary For Cybersecurity working alongside another assistant secretary focused on the protection of the physical structure while remaining integrated under an Under Secretary for IAIP.

It is particularly important that the Assistant Secretary for Cybersecurity have primary authority over the National Communications System, which is, of course, included in this bill. This is important given the convergence of data and voice networks.

As you know, the National Communications System has control over priority communications. These networks proved critical in the immediate aftermath of 9/11. CSIA strongly believes that the government needs a comprehensive approach to cybersecurity, and by establishing assistant secretary, we can do much better than we are today.

I think there are three documents that we could look at that set out the government's overall policy or the administration's policy in cybersecurity. The first is the President's National Strategy, the second is Homeland Security Presidential Directive Number 7, and the third is the National Response Plan.

There are some common characteristics among those documents. I think in the first instance, it is worthwhile pointing out that these documents bound, if you will, the responsibilities of DHS—they don't, and DHS too, if you will, boil the ocean. They bound their responsibilities in the area of creating an emergency communications network in case of an attack, to prepare contingency plans in the case of an attack, to carefully look at reconstitution issues in case of an attack, to look at early warning issues; for example, if the government has the means to understand through intelligence assets that might be overseas or here, to pass that information on to the private sector, and it might not be readily available to the private sector. Those are private tasks that the Department of Homeland Security has been given under the three documents I mentioned.

The progress to date at the Department has not been what you would hope. They have a myriad of programs set up, wonderful intentions, but at the end of the day, they are not succeeding in those very critical tasks that are so important to our economic and national security.

If I were to prioritize those tasks, they would be just as I have outlined. It would be simply working on to identify and prioritize critical infrastructure related to information systems, prepare for contingencies by ensuring that we have survivable communications in place, work closely with the private sector on any sort of reconstitution plans that need to be put in place, provide warning of disruption, provide early warning of an attack through intelligence means. These tasks can really only be effectively done at the assistant secretary level or higher. They cannot be done at a lower level.

I want to speak very quickly, before I close, on the difference between cyber and physical infrastructure. By advocating for an Assistant Secretary of Cybersecurity, we are not dismissing the need to integrate cyber and physical infrastructure protection, nor are we saying that the protection of cyberinfrastructure is more important than the protection of physical infrastructure. Although it is—increasingly the IT infrastructure is a critical component in the operation of our physical infrastructures.

Cyberinfrastructure is attacked and defended differently than the physical infrastructure. Cyberinfrastructure is largely defended by technical specialist, not through guns, gates, guards and cameras. Vulnerabilities are discovered through technical means and often require immediate remediation involving a variety of parties across different sectors of the economy.

A cyberattack may be launched remotely, requiring no physical access to a target. Cyberattacks may not necessarily be abrupt. For instance, a cyberattack may be low and slow, changing or otherwise corrupting political data over an extended period of time.

The infrastructure is dynamic, constantly changing. Amit and Harris have addressed this. But I want to point out also, in the event of an event of national significance affecting one or more sectors across the economy, we are going to turn to our information systems to help bail us out.

The National Communications System post-9/11 helped us in that environment. By the way, the National Communications System under DOD was run by a lieutenant general. Now we are at an acting—acting director level. It is important that we have an assistant secretary in place as soon as possible. During Q and A I would be happy to speak to source issues.

Thank you.

Mr. LUNGREN. Thank you very much, Mr. Kurtz.

[The statement of Mr. Kurtz follows:]

PREPARED STATEMENT OF PAUL B. KURTZ

Thank you, Chairman Lungren and Ranking Member Sanchez for inviting the Cyber Security Industry Alliance (CSIA) to testify before this subcommittee in reference to HR 285. I would also like to acknowledge Congressman Thornberry and Congresswoman Lofgren for their continued efforts in support of an Assistant Secretary for Cyber Security position in DHS. Their bi-partisan work is evident in their co-sponsorship of this bill.

As Executive Director of CSIA, I am pleased to speak about the need for an Assistant Secretary for Cyber Security in the Department of Homeland Security. CSIA supports rapid passage of HR 285.

The members of the Business Software Alliance also support this legislation and I am also speaking on their behalf.

Since the late 1990s, we have spoken of a "partnership" to secure the critical infrastructure of the United States, particularly the information infrastructure, since it is owned and operated by the private sector. For this partnership to truly be successful and not simply rhetoric, we need a clear leader in the Department of Homeland Security to act as a focal point for this partnership. A Director-level position does not have the sufficient stature or programmatic authority for accountability, or to reach across sectors. A leader in securing the critical infrastructure must have the authority and resources to accomplish this important and complex mission.

This leader must be at least at the Assistant Secretary level to have the impact that is needed.

Unlike other sectors, the information infrastructure is dynamic and will continue to evolve for the foreseeable future. Changes within the information infrastructure are driving change in all other sectors. Cyber and physical infrastructure security will receive greater respective attention with an Assistant Secretary for Cyber Security working alongside the Assistant Secretary for Infrastructure Protection, while remaining integrated under the leadership of the Undersecretary for Infrastructure Protection and Information Analysis. It is particularly important that the Assistant Secretary for Cyber Security have primary authority over the National Communications System, given the convergence of voice and data networks.

CSIA strongly believes that the Federal government needs a comprehensive approach to cyber security protection. The establishment of an Assistant Secretary for Cyber Security in the Department of Homeland Security is a critical initial step in this approach.

I will cover three areas in my testimony:

- A brief introduction to CSIA
- An overview of the roles and responsibilities of the Department of Homeland Security in the area of cyber security
- The importance of clear leadership on the issue of cyber security

Introduction to CSIA

CSIA is dedicated to enhancing cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment be-

hind emerging industry technology standards and public education. CSIA is the only CEO-led public policy and advocacy group exclusively focused on cyber security policy issues. We believe that ensuring the security, integrity and availability of global information systems is fundamental to economic and national security. We are committed to working with the public sector to research, create and implement effective agendas related to national and international compliance, privacy, cybercrime, and economic and national security. We work closely with other associations representing vendors as well as critical infrastructure owners and operators, as well as consumers.

Members of the CSIA include BindView Corp; Check Point Software Technologies Ltd.; Citadel Security Software Inc.; Citrix Systems, Inc.; Computer Associates International, Inc.; Entrust, Inc.; Internet Security Systems Inc.; iPass Inc.; Juniper Networks, Inc.; McAfee, Inc; PGP Corporation; Qualys, Inc.; RSA Security Inc.; Secure Computing Corporation; Symantec Corporation and TechGuard Security, LLC.

CSIA understands that the private sector bears a significant burden for improving cyber security. CSIA embraces the concept of sharing that responsibility between information technology suppliers and operators to improve cyber security. Cyber security also requires non-partisan government leadership. Work to strengthen cyber security began in the Clinton administration. The Bush administration has continued and boosted this work, through the creation of the National Strategy to Secure Cyberspace. The National Strategy remains timely and salient.

Roles and Responsibilities

Last December, the Cyber Security Industry Alliance released an agenda for the administration that outlined twelve steps to help build a more secure critical infrastructure that called for an Assistant Secretary level post in the Department of Homeland Security. To understand why we feel this is critically important to the protection of our cyber infrastructure, I thought it would be helpful to expand on the Agenda and offer a framework to help define Federal versus private sector responsibilities in the area of cyber security.

By outlining the responsibilities of the Department of Homeland Security in the area of cyber security, we feel that the need for an Assistant Secretary-level position can be better understood.

Three Federal documents provide a framework for Federal responsibilities to secure cyberspace:

- The President's National Strategy to Secure Cyberspace (February 14, 2003)
- Homeland Security Presidential Directive-7 (December 17, 2003)
- The National Response Plan's Cyber Incident Annex (January 6, 2005)
- President's National Strategy to Secure Cyberspace

The President's National Strategy is an appropriate place to start. While the Strategy's recommendations receive substantial attention, it also provides clear policy guidance on the Federal government's role. The President's cover letter for the Strategy states:

"The policy of the United States is to protect against the **debilitating disruption** of the operation of information systems for critical infrastructures and, thereby help to protect the people, economy, and national security of the United States." He continues, "We must act to reduce our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our nation's *critical infrastructure* and ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable and cause the least damage possible."

The strategy adds some additional guidance on its role, noting that it is appropriate for the government to assist with forensics, attack attribution, protection of networks and systems critical to national security, indications and warnings, and protection against *organized attacks* capable of inflicting *debilitating* damage to the economy.

Additionally, Federal activities should also support research and development that will enable the private sector to better secure privately-owned portions of the nation's critical infrastructure.

These statements lead to the conclusion that Federal activity is bounded to protecting against **debilitating** attacks against **critical infrastructure,** attack attribution for national security systems, forensics and research and development.

The Strategy also sets specific responsibilities for Federal agencies, including the Department of Homeland Security. The Strategy states that the Department should:

- Develop a comprehensive plan to secure critical infrastructure.
- Provide crisis management and technical assistance to the private sector with respect to recovery plans for failures of critical information systems
- Coordinate with other Federal agencies to provide specific warning information and advice about appropriate protective measures and countermeasures to

state, local and nongovernmental organizations including the private sector, academia and the public

• Perform and fund research and development along with other agencies that will lead to new scientific understanding and technologies in support of homeland security.

It is important to note that the Strategy does not place responsibility for every problem associated with cyber security with DHS, but focuses its role on contingency planning and emergency communications—two critical areas of defense against threats to our national security.

HSPD–7

HSPD–7 establishes the U.S. government's policy for the identification and protection of critical infrastructure from terrorist attacks. It advances the President's strategy in a number of areas and helps further refine the Federal government's role in securing cyberspace.

HSPD–7 focuses in large part on the identification and protection of assets that if attacked would cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction. It also addresses the protection of infrastructure that if attacked would:

• Undermine state and local government capacities to maintain order and to deliver minimum essential public services.

• Damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services

• Have a negative effect of the economy through the cascading disruption of other critical infrastructure and key resources.

• Undermine the public's morale and confidence in our national economic and political institutions.

HSPD–7 designated the Department of Homeland Security as a focal point for information infrastructure protection, including cyber security, stating:

11The Secretary will continue to maintain an organization to serve as a focal point for the security of cyberspace. The organization's mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems."

The National Response Plan's Cyber Incident Annex

The National Response Plan (NRP) upholds the President's National Strategy to Secure Cyberspace and HSPD–7. The NRP Cyber Incident Annex states that the Federal government plays a significant role in managing intergovernmental (Federal, state, local and tribal) and, where appropriate, public-private coordination in response to cyber incidents of *national significance.*

A Framework for Federal Action

The President's National Strategy to Secure Cyberspace, Presidential Directive 7 and the National Response Plan yield a possible two-tier framework for Federal responsibility.

Tier One—Functions Critical to U.S. Economic and National Security

1. Identify and prioritize critical information infrastructure that if disrupted would have a debilitating impact on critical infrastructure or systems essential to U.S. economic or national security

2. Prepare for such contingencies by ensuring survivable communications networks among key critical information infrastructure operations in the government and private sector

3. Prepare contingency plans in the event of a disruption that include crisis management and restoration of critical networks, and regularly exercise, test and refine these plans.

4. Provide warning of attack or disruption to critical infrastructure owners and operators from resources or capabilities that are not available to the private sector through such means as intelligence.

Tier Two—Supporting Functions that Improve Coordination, Awareness, Education and Personnel Readiness

1. Facilitate coordination between individual sectors of the economy by establishing appropriate government advisory committees

2. Facilitate and support general awareness among all information system users, including home users and small businesses

3. Track trends and costs associated with information infrastructure attacks and disruptions, through such means as U.S. CERT.

4. Coordinate and support long-term research and development for cyber security.

The Importance of Clear Leadership on the Issue of Cyber Security

When you look closely at the responsibilities of The Department of Homeland Security in the area of cyber security, you see that while it may be narrowly defined, its responsibilities are extremely significant to our economic and national security. **DHS is the government's focal point for the prevention, response and recovery from cyber security incidents that have a debilitating impact on our national and economic security.** While the private sector has a critical role to play in the protection of critical information infrastructure, DHS serves as the government's and nation's point of coordination for all our efforts. Senior DHS leadership is needed to build an effective government-private sector relationship, to understand the technical and global complexities of cyber security, and to marshal the resources necessary to provide an effective partnership with private sector organizations and initiatives.

Cyber vs. Physical Infrastructure Protection

By advocating for an Assistant Secretary for Cyber Security, we are not dismissing the need to integrate cyber and physical infrastructure protection. Nor are we saying that the protection of the cyber infrastructure is more important than the protection of the physical infrastructure—although it is increasingly a critical component in the operation of our physical infrastructures, and in fact, it cuts across all of our physically infrastructures. The physical and cyber infrastructures are related, but they are fundamentally different in a variety of ways. For example:

- Cyber infrastructure is attacked and defended differently than the physical infrastructure. Cyber infrastructure is largely defended by technical specialists, not through guns, gates, guards, and cameras. Vulnerabilities are discovered through technical means and often require immediate remediation involving a variety of parties across different sectors of the economy. A cyber attack may be launched remotely, requiring no physical access to a target. Cyber attacks may not necessarily be abrupt. For example, a cyber attack may be "low and slow," changing or otherwise corrupting critical data over an extended period of time.
- Cyber infrastructure is dynamic, where the physical infrastructure is more static. For example, power plants, power lines, chemical plants, railroads, bridges remain stationary with more gradual changes in technology, where information networks are rapidly changing. An IP-based transaction may traverse the globe via satellite, wireless, or terrestrial cable. The technologies that support these different means are changing rapidly.

In an event of national significance affecting one or more of the physical infrastructures, the cyber infrastructure takes on additional responsibility for ensuring we have the ability to coordinate and respond to attacks. Our IT infrastructure is operational; without it, our national response capability is crippled.

We believe it is appropriate to have an Assistant Secretary for Cyber Security working along side an assistant secretary responsible for securing the physical infrastructure under the leadership of an Under Secretary as proposed in H. 285.

Conclusion

Mr. Chairman, we are seeing increased threats and vulnerabilities associated with our information infrastructure. We rely upon our information infrastructure, yet there is no one clearly in charge of coordinating its security and reliability. Presidential guidance and the Homeland Security Act clearly identify the Department of Homeland Security as the most appropriate focal point for coordinating the protection of our information infrastructure. We strongly support HR 285 and its creation of a more senior position at DHS to lead efforts to build a more secure information infrastructure for both the government and private sector.

Mr. LUNGREN. The Chair now recognizes Catherine Allen, president and CEO of BITS, a division of the Financial Services Roundtable, to testify.

STATEMENT OF CATHERINE ALLEN, PRESIDENT AND CEO, BITS, FINANCIAL SERVICES ROUNDTABLE

Ms. ALLEN. Thank you very much. Thank you, Chairman Lungren and committee members, for the opportunity to testify before the committee. We commend Congressman Thornberry and Congresswoman Lofgren on the bill.

I am Catherine Allen, CEO of BITS, a nonprofit industry consortium of the largest 100 financial institutions in the U.S. We are a

nonlobbying division of the Financial Services Roundtable. Our mission is to serve the financial services needs at the interface between commerce, technology and financial services. We work with government organizations, DHS, Treasury, Federal financial regulators, the Federal Reserve and other technology associations.

Given the short amount of time, I want to focus on three major points today: First, the state of cybersecurity; second, reasons in favor of elevating the cybersecurity position at DHS; and third, steps the government could take to strengthen cybersecurity.

My written statement contains additional information on BITS, cybersecurity, crisis management, critical infrastructure, management of outsources and fraud reduction efforts. It also contains suggestions that BITS has given to DHS in the past, as well as others on how to strengthen cybersecurity.

The importance of cybersecurity cannot be overstated. Our Nation's economic and national security relies on the security, reliability, recoverability, continuity and maintenance of information systems. The security and reliability of the information systems are increasingly linked to consumer and investor confidence.

As I speak, criminals are writing code to compromise systems. Viruses are epidemic. Hackers are closing the window between the discovery of a flaw and the release of a new virus, now an average of 5.8 days. Over 1,200 new security flaws were discovered just in the last 6 months of 2004.

Beyond threats to our Nation's infrastructure, leaders in the financial services industry are growing increasingly concerned about the impact on consumer confidence. As one example, fraudsters are finding new ways to trick consumers in providing initial information that can facilitate ID theft through phishing, pharming and other e-scams.

The financial services industry has been aggressive in its efforts to strengthen cybersecurity and reduce fraud. We are sharing information; analyzing threats; creating best practices; urging the software and technology providers to do more to secure their products and services, something we call a higher duty of care; and combating fraud and identity theft.

Just last week BITS and the Roundtable announced the permanent creation of an Identity Theft Assistance Center, a free service to financial institution customers that helps victims restore their financial identity. The ITAC has helped, to date, nearly 700 consumers restore their financial identities since it became operational last August. The ITAC information is shared with law enforcement to help prosecute the perpetrators, and the ITAC is the cornerstone of a broader industry effort to detect and prevent fraud, help victims address the causes of identity theft and prosecution of fraudsters.

In a related effort, BITS created a phishing prevention and investigation network, again helping our industry to shut down online scams and aid in investigating perpetrators and providing a united front with law enforcement.

Last year I submitted a letter in support of a proposal to elevate the position of Cybersecurity Director at the Department of Homeland Security to the assistant secretary level. We support rapid passage of H.R. 285. Cybersecurity is handled in DHS at a level far

below where most financial services corporations handle the issues today, and that is at the board-room level. Elevating this critical position and insuring that adequate funding is provided will help us to focus greater attention on cybersecurity issues within the government and provide a more senior-level dialogue with the private sector. It will enable implementation of many key elements that were identified in the administration's National Strategy to Secure Cyberspace.

Much of the focus at DHS has been on physical security. While that is important, we believe there are several areas that need much more focus. It starts with cybersecurity, but also a means addressing the interdependencies between our sector and other critical infrastructures, including the telecommunications and power industries. They, too, rely and need a strengthened cybersecurity effort. Elevating the cybersecurity position within DHS should be a first significant step as part of a broader strategy to strengthening cybersecurity.

For the record, it is important for the committee to understand that the financial regulators are taking cybersecurity issues seriously. Treasury is a sector leader. DHS plays an important role in bringing the other sectors along in addressing the cybersecurity issues.

We believe that there is much more that can be done to strengthen cybersecurity. My written statement includes a more detailed review of seven key elements that the Federal Government should support to ensure information technology security. I refer to them by the acronym PREPARE.

The first is promote, playing an important role of promoting the importance of secure information technology and in facilitating collaboration.

The second is responsibility, promoting shared responsibility between the suppliers and the end users for developing, deploying and maintaining secure information software and networks.

The third is educate. All sectors should make it a priority to communicate to all users of information technology the importance of safe practices.

The fourth is procure, using its purchasing power to leverage security requirements, such as software testing. Along with employing best practices developed by public and private sectors, the government can play an important role in encouraging the changes that need to take place.

The fifth is analyze. Government should collect and provide to the critical infrastructures and policymakers the kinds of statistics we need on threats, risks and vulnerabilities.

The next to last is research. The government can play an important role in funding R&D in the development of more secure software development practices, testing and certification programs.

Lastly, enforce. Law enforcement must do more to enforce, investigate and prosecute cybercrimes here and abroad. E-crimes are growing and undermine our economy. Law enforcement must have the resources and mandate to go forward.

In conclusion, the financial services sector is a key part of the Nation's critical infrastructure. Customer trust in the security of financial transactions is vital to the security of not only the infra-

structure, but the strength of the Nation's economy. Our sector is a target of cybercriminals as well as terrorists. We have a vested interest in this being raised to a higher level of dialogue in the community.

We have taken major strides to respond to the risks that we have today. We need the government to support these efforts, to support cybersecurity, with the same level of the energy, resources and stature as protecting physical security through DHS. Elevating the cybersecurity position to an assistant secretary level is a step in the right direction, but there is much more that is needed.

Thank you for the opportunity to testify.

Mr. LUNGREN. Thank you very much, Ms. Allen.

[The statement of Ms. Allen follows:]

PREPARED STATEMENT OF CATHERINE A. ALLEN

Introduction

Thank you, Chairman Lungren and Ranking Member Sanchez, for the opportunity to submit testimony before the House Committee on Homeland Security's Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity about proposed legislation to elevate the Cyber Security Director at the Department of Homeland Security (DHS) to the Assistant Secretary level.

I am Catherine Allen, CEO of BITS, a nonprofit industry consortium of 100 of the largest financial institutions in the U.S. BITS is the non-lobbying division of The Financial Services Roundtable. BITS' mission is to serve the financial services industry's needs at the interface between commerce, technology and financial services. BITS members hold about $9 trillion of the nation's total managed financial assets of about $18 trillion. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect. BITS' activities are driven by the CEOs and their direct reports—CIOs, CTOs, Vice Chairmen and Executive Vice President-level executives of the businesses. BITS works with government organizations including the U.S. Department of Homeland Security, U.S. Department of the Treasury, federal financial regulators, Federal Reserve, technology associations, and major third-party service providers to achieve its mission. Attached to this statement is an overview of our work related to cyber security, crisis management coordination, critical infrastructure protection, and fraud reduction.

The importance of cyber security cannot be overstated. Our nation's economic and national security relies on the security, reliability, recoverability, continuity, and maintenance of information systems. IT security has a direct and profound impact on the government and private sectors, and the nation's critical infrastructure. Further, the security and reliability of information systems is increasingly linked to consumer and investor confidence.

As I speak, hackers are writing code to compromise systems. Viruses are epidemic. Hackers are closing the window between the discovery of a flaw and the release of a new virus. Fraudsters are finding new ways to trick consumers into providing personal information that can facilitate ID theft. Beyond threats to our nation's infrastructure, leaders in the financial services industry are growing increasingly concerned with the impact on consumer confidence.

The financial services industry has been aggressive in its efforts to strengthen cyber security. We are sharing information, analyzing threats, urging the software and technology industries to do more to provide more secure products and services, and combating fraud and identity theft. Just last week, BITS and The Roundtable announced the results of a pilot of the Identity Theft Assistance Center (ITAC). The ITAC has helped nearly 700 consumers restore their financial identities since it became operational last August. The ITAC is a free service to financial institution customers. It is a key part of industry efforts to help victims and address the causes of identity theft.

Last year I submitted a letter in support of a proposal to elevate the position of Cyber Security Director at the Department of Homeland Security to the Assistant Secretary level (Attachment A).

BITS and The Financial Services Roundtable support this effort to increase the administration's focus on cyber security concerns and address our sector's concerns. While much of DHS' focus has been on physical security, it has not focused enough attention on addressing cyber security concerns. Elevating the cyber security posi-

tion is a small step as part of a broader strategy to strengthen cyber security. Cyber security is handled at a level far below where most corporations handle the issues today. Elevating this critical position and ensuring that adequate funding is provided will help to focus greater attention on cyber security issues within the government and throughout the private sector and thus implement many areas identified in the Administration's National Strategy to Secure Cyberspace.

Since the creation of DHS in March 2003, BITS has worked closely with many DHS officials, including the director and acting director of the Cyber Security Division. We have provided numerous suggestions for DHS actions to strengthen cyber security and ways it can work in partnership with leaders in the private sector. Earlier this year, the National Cyber Security Division convened a "retreat" of representatives from the major associations (e.g., BITS, Center for Internet Security, Cyber Security Industry Alliance, Educause, Information Technology Association of America, ISAlliance, Technet, SANS Institute, U.S. Chamber of Commerce), individual companies (e.g., IBM, Microsoft, RSA), law enforcement (e.g., Federal Bureau of Investigations, U.S. Secret Service) and government (e.g., Central Intelligence Agency, Commerce Department, Defense Department, Homeland Security Department, House of Representatives, Justice Department, Treasury Department, National Security Agency). DHS played an important leadership role in convening the meeting and other meetings of the US-CERT program. Attachment B is a summary of answers to several questions DHS officials asked in advance of the meeting.

More Can Be Done

As an organizational and symbolic step, elevating this critical position will help to focus greater attention on cyber security issues within the government and throughout the private sector.

However, this should be viewed as just one of many steps that must be taken to strengthen cyber security.

Government plays an enormous role. Our nation's economic and national security relies on the security, reliability, recoverability, continuity, and maintenance of information systems. IT security has a direct and profound impact on the government and private sectors, and the nation's critical infrastructure. Further, the security and reliability of information systems is increasingly linked to consumer and investor confidence. In recent years, members of the user community that rely on technology provided by the IT industry—private-sector companies, universities and government agencies—are demanding greater *accountability* for the security of IT products and services.

PREPARE

The federal government can play an important role in protecting the nation's IT assets. The following are seven key elements that the U.S. government should support to secure information technology.

Promote. Government can play an important role in promoting the importance of secure information technology. Also, government should do more to facilitate collaboration among critical infrastructure sectors and government. Some sectors, such as financial services, are heavily regulated and supervised to ensure that customer information is protected and that financial institutions operate in a safe and sound manner. Examples of actions the government can take include:

- Government should lead by example by ensuring that the issue of cyber security receives adequate attention in the Department of Homeland Security. Today, cyber security is handled at a level far below where most corporations handle these issues. Congress could create a more senior-level policy level position within DHS to address cyber security issues and concerns and ensure that adequate funding is provided.
- Strengthen information sharing coordination mechanisms, such as the Information Sharing and Analysis Centers (ISACs), by ensuring adequate funding is made available to Federal agencies sponsoring such organizations. Information sharing and trend analysis within a sector is essential to protecting information security and responding to events. Information sharing among sectors is equally important as cyber threats sometimes reach some sectors before others.
- Create an emergency communication and reconstitution system in the event of a major cyber attack or disruption of information networks. Such an attack or disruption could potentially cripple many of the primary communication channels. To allow maximum efficiency of information dissemination to key individuals in such an event, a thorough and systematic plan should be in place. The financial services industry has developed such a plan for industry-specific events in the BITS/FSR Crisis Communicator. Other organizations have developed similar communication mechanisms. These emergency communications

programs should be examined as potential models for a national cyber security emergency communication system.

• Reform of the Common Criteria/National Information Assurance Partnership (NIAP). The current software certification process is costly, inefficient, used on a limited basis by the Federal government, and virtually unknown to the private sector. NIAP should be reformed so that it is more cost effective for vendors to seek certification while ensuring consistent Federal procurement practices and expanded commercial adoption of NIAP-certified products. The BITS Product Certification Program may well be able to serve as a model.

Responsibility. Government should promote shared responsibility between suppliers and end users for developing, deploying, and maintaining secure information networks. Government can play an important role in establishing incentives and making producers of software and hardware accountable for the quality of their products. Examples of actions the government can take include:

• Provide tax or other incentives for achieving higher levels of Common Criteria certification. Incremented incentives would help to compensate companies for the time and cost of certification. This should encourage certification and increase the overall security of hardware and software.

• Provide tax or other incentives for certification of revised or updated versions of previously certified software. Under Common Criteria, certification of updated versions is costly and time consuming. Incentives are necessary to ensure that all software is tested for security

• Require software providers to immediately notify ISACs of newly discovered cyber threats and to provide updated information on such threats until an effective patch is provided. It is vital that critical infrastructure companies receive immediate notice of serious vulnerabilities.

• Establish requirements that improve the patch-management process to make it more secure and efficient and less costly to organizations.

Educate. Communicate to all users of information technology the importance of safe practices. Public confidence in e-commerce and e-government is threatened by malicious code vulnerabilities, online fraud, phishing, spam, spyware, etc. Ensuring that users (home users, businesses of all sizes, and government) are aware of the risks and take appropriate precautions is an important role for government and the private sector. Examples of actions the government can take include:

• Fund joint FTC/DHS consumer cyber security awareness campaign. The FTC should focus its efforts on building consumer awareness, and DHS should coordinate more detailed technical education regarding specific serious threats. In addition, government employees should be trained in proper cyber safety measures.

• Train government employees on proper cyber security measures.

• Educate corporate executives and officers regarding their duties under Sarbanes-Oxley, GLBA, and HIPAA as they relate to cyber security.

Procure. Using its purchasing power and leveraging security requirements and best practices developed by the public and private sectors, government can play an important role in encouraging the IT industry to deliver and implement more secure systems. Examples of actions the government can take include:

• Require high levels of cyber security in software purchased by the government through procurement procedures. Extend such requirements to software used by government contractors, subcontractors, and suppliers.

• Provide NIST with adequate resources to develop minimum cyber security requirements for government procurement. NIST should include software developers and other stakeholders in the standard-creation process.

Analyze. Government should collect information and analyze the costs and impact of information security risks, vulnerabilities and threats and provide this analysis to policy makers. Examples of actions the government can take include:

• Assign to the Commerce Department or another appropriate agency the responsibility of tracking and reporting such costs and their impact on the economy. Measuring and making these costs transparent will aid law makers and regulators as they assign resources to cyber security programs.

Research. Government can play an important role in funding R&D in the development of more secure software development practices, testing and certification programs. In addition, training future generations of programmers, technicians and business leaders that understand and manage information security can be accomplished by establishing university and educational/certification programs. Government can help by facilitating collaboration with the users and suppliers of IT to de-

velop standards for safe practices. Examples of actions the government can take include:

- Enhance DHS, NSF, and DARPA cyber security R&D funding.
- Carefully manage long- and short-term R&D to avoid duplication.
- Establish a mechanism to share educational training and curricula.

Enforce. Law enforcement must do more to enforce, investigate and prosecute cyber crimes here and abroad. Examples of actions the government can take include:

- Ratify the Council of Europe's Convention on Cybercrime.
- Enhance criminal penalties for cyber crimes.
- Make cyber crimes and identity theft enforcement a priority among law enforcement agencies.
- Encourage better coordination among law enforcement agencies in order to detect trends.

The Financial Services Industry Is Leading the Way in Responding to the Cyber Security Challenge

The financial services sector is a key part of the nation's critical infrastructure. Customer trust in the security of financial transactions is vital to the stability of financial services and the strength of the nation's economy. At the same time, our sector is a favorite target of cyber criminals as well as of terrorists, as was made clear on 9/11.

Since 9/11, the financial services sector has taken major strides to respond to the risks we face today. BITS has made coordinating financial services industry crisis management efforts a top priority. Senior executives at our member companies have dedicated countless hours to preparing for the worst. We have convened numerous conferences and meetings to bring together leaders and experts, developed emergency communication tools, strengthened our sector's Information Sharing and Analysis Center (FS/ISAC), conducted worst case scenario exercises, engaged in partnerships with the telecommunications sector and key software providers, compiled lessons learned from 9/11 and the August 2003 blackout, developed best practices and voluntary guidelines, created a model for regional coalitions, developed liaisons and pilots with the telecommunications industry for diversity and redundancy, and combated new forms of online fraud. Additionally, BITS is now developing best practices in collaboration with the electric power industry.

Lessons Learned

BITS regularly gathers and disseminates "lessons learned" from its membership. These lessons are a critical building block for BITS' best practices. Below are some of those lessons for the Committee to consider.

We must work with other parties in the private and public sectors to address these issues sufficiently. We understand that the risks for national security and economic soundness cannot be underestimated. Neither can the importance of our working together to address them.

We need to look strategically and holistically at the nation's critical infrastructures and what can be done to enhance resiliency and reliability. We urge the Committee to consider all aspects of critical infrastructure—the software and operating systems, the critical infrastructure industries, and the practices of firms, industries and the government—in addressing software security and vulnerability management.

Preparation is critical. The events of 9/11 and subsequent preparations by the private sector and government enhanced mutual trust and the ability to communicate, shift to backup systems, and continue operations. Prior to the August 2003 blackout, BITS conducted a scenario exercise that included the West Coast power grid being out for seven days and the impact that might have on the sector. That exercise helped the industry think through things like communications, water shortages, backup for ATM operations, and fuel for generators.

Critical infrastructure industries and the public need to have an understanding of the scope and cause as early as possible when a major event occurs. During the August 2003 blackout, the announcement that the problem was not the result of a terrorist event alleviated public concerns and made for orderly execution of business continuity processes. If it had been a terrorist event, other communications and directives such as "shields up"—in which external communications to institutions are blocked—might have occurred.

Diverse and resilient communication channels are essential. Diverse elements—such as cell phones, wireless email devices, landline phones, and the Internet—are required. Both diversity and redundancy are needed within critical infrastructures to assure backup systems are operable and continuity of services will be maintained.

The power grid must be considered among the most vital of critical infrastructures and needs investment to make sure it works across the nation. The cascading impact on the operation of financial services, access to fuel, availability of water, and sources of power for telephone services and Internet communications cannot be overstated.

Recognize the dependence of all critical infrastructures on software operating systems and the Internet. A clear understanding of the role of software operating systems and their "higher duty of care," particularly when serving the nation's critical infrastructures, needs to be explored. Further, the Committee should recognize that the financial sector is driven by its "trusted" reputation as well as regulatory requirements. Other industries do not have the same level of regulatory oversight, liability, or business incentives. However, we rely on other sectors because of our interdependencies. Responsibility and liability need to be shared.

Financial Industry Efforts to Strengthen Cyber Security

In October 2003, BITS began its Software Security and Patch Management initiative to respond to increasing security risks and headline-sweeping viruses. Since then, BITS has worked to mitigate security risks to financial services consumers and the financial services infrastructure, ease the burden of patch management caused by vendor practices, and help member companies comply with regulatory requirements. BITS also began forging partnerships with the software vendors most commonly used in our industry.

In February 2004, BITS and The Financial Services Roundtable held a Software Security CEO Summit. The event launched BITS and Roundtable efforts to promote CEO-to-CEO dialogue on software security issues. More than 80 executives from financial services, other critical infrastructure industries, software companies, and government discussed software vulnerabilities and identified solutions. A "toolkit" with software security business requirements, sample procurement language, and talking points for discussing security issues with IT vendors was distributed to 400 BITS and Roundtable member company executives. One important deliverable from this Forum is the set of Software Security Business Requirements, which are essential from the perspective of the financial services sector. These requirements and the full "toolkit" are available in the public area of the BITS website, at *www.bitsinfo.org.*

A theme of the event was the importance of collaborating with other critical infrastructure industries and government. Since the Summit we have worked with all the associations representing the financial services industry, as well as The Business Roundtable, the Cyber Security Industry Alliance and other relevant groups.

In April 2004, BITS and The Financial Services Roundtable announced a joint policy statement calling on the software industry to improve the security of products and services it provides to financial services customers. The policy statement calls on software providers to accept responsibility for their role in supporting financial institutions and other critical infrastructure companies. BITS and The Roundtable support incentives and other measures that encourage implementation of more secure software development processes and sustain long-term R&D efforts to support stronger security in software products. We also support protection from antitrust laws for critical infrastructure industry groups to discuss baseline security specifications for the software and hardware that they purchase. Additionally, as part of the policy, BITS and The Roundtable are encouraging regulatory agencies to explore supervisory tools to ensure critical third-party service providers and software vendors deliver safe and sound products and services to the financial services industry.

We continue to work with software companies to create solutions acceptable to all parties. In 2004 BITS successfully negotiated with Microsoft to provide additional support to BITS member companies using Windows NT. We have provided Microsoft and other software and hardware companies with Software Security Business Requirements. (See Attachment A.) BITS members agree that these requirements are critical to the soundness of systems used in the financial services industry.

In July 2004, BITS published best practices for software patch management in response to the increasing urgency of patch implementation, given the speed with which viruses are targeting new vulnerabilities. This document is available to the public at no cost and applicable to industries outside of financial services.[1]

In July, BITS published *The Kalculator: BITS Key Risk Measurement Tool for Information Security Operational Risks.* This tool helps financial institutions evaluate

[1] Patch management and implementation alone can cost one financial institution millions of dollars annually. A BITS survey of member institutions found that costs to the financial services industry associated with software security, including patch management, are approaching $1 billion annually. BITS' best practices help companies mitigate these costs.

critical information security risks to their businesses. Financial institutions use the *Kalculator* to score their own information security risks based on the likelihood of an incident, the degree to which the organization has defended itself against the threat, and the incident's possible impact. The tool brings together an extensive body of information security risk categories outlined in international security standards and emerging operational risk regulatory requirements. Like the patch management best practices, the *Kalculator* is available to the public at no cost and applicable to industries outside of financial services.

BITS participated in the Corporate Information Security Working Group (CISWG) sponsored by Congressman Adam Putnam, then-Chairman of the House of Representatives' Subcommittee on Technology, Information Policy, Intergovernmental Relations on the Census. CISWG is made up of corporate, industry and academic leaders and is working to pursue a private sector-driven approach to enhancing the protection of the nation's corporate computer networks. BITS is active in the best practices, incentives, and procurement subgroups. In addition, BITS has participated in task forces established by DHS and several technology associations.

Finally, the BITS Product Certification Program is another important part of our work to address software security. The BITS Product Certification Program is a testing capability that provides security criteria against which software can be tested. A number of software companies are considering testing. The criteria are also used by financial institutions in their procurement processes. We are working to hand this over to DHS and secure ongoing funding for it.

Identity Theft and Phishing: Prevention and Victim Assistance

Just as financial institutions are a key target for hackers and other cyber criminals, our industry is increasingly the target of fraudsters operating online. BITS and The Financial Services Roundtable are responding to the escalation in identity theft with a series of steps to facilitate prevention of the crime and assist victims when it occurs. The goals of these efforts are to help maintain trust in the financial services system, assist member companies' customers, and mitigate fraud losses. BITS and The Roundtable are working with the Administration, Congress, and law enforcement and regulatory agencies to accomplish these goals.

A cornerstone to these efforts is the Identity Theft Assistance Center (ITAC). Developed by BITS and The Roundtable, with the support of 50 founding member institutions, the ITAC helps victims of identity theft restore their financial identity. If a consumer or a member company suspects a problem, the consumer and the company resolve any issues, and if the problem involves identity theft, the customer is offered the ITAC service. The ITAC walks the consumer through his or her credit report to find any other suspicious activity. Then, the ITAC notifies the affected creditors and places fraud alerts with the credit bureaus. The ITAC also shares information with the Federal Trade Commission and law enforcement agencies, to help arrest and convict the perpetrators and prevent future identity theft crimes.

Because a consistent understanding of the problem is essential to finding solutions, a 2003 BITS white paper on identity theft outlines the full identity theft landscape, establishing key terms as well as identifying factors that contribute to identity theft. The paper provides background about the legislative and policy environment, including existing and proposed laws, as well as industry best practices.

Along with the white paper, BITS developed guidelines for financial institutions to use to prevent identity theft and restore victims' financial identities. The guidelines include processes for providing a "single point of contact" at companies to whom victims may report cases of identity theft.

Additionally, the BITS Fraud Reduction Steering Committee and the Federal Trade Commission have created a Uniform Affidavit to simplify the recovery process for victims. The Uniform Affidavit streamlines the reporting process by recording the victim's information about the crime, so that victims only have to tell their story once.

BITS is also responding to "phishing" through its Fraud Reduction Program. Phishing is the practice of luring consumers to provide bank account and other personal information to fraudsters through bogus email messages. In response to these and other online scams, BITS has created a Phishing Prevention and Investigation Network. The Phishing Network provides member institutions with information and resources to expedite investigations and address phishing/spoofing incidents. The Phishing Network includes a searchable database of information from financial institutions on their phishing incident and response experience, including contacts at law enforcement agencies, foreign governmental agencies, and ISP Web administrators. The Phishing Network also provides data on trends to help law enforcement build cases and shut down identity theft operations.

Financial institutions are regulated to "know your customers." However, financial institutions currently do not have access to various government databases to validate information provided at new account openings. For instance, financial institutions cannot validate that a passport number belongs to the individual providing it and matches the address given at a new account opening. This is also true of driver's license and tax ID numbers. (A pilot is underway with Social Security numbers; BITS is hopeful that financial institutions will finally be able to validate Social Security numbers.) Financial institutions do not want direct access to the information; they would like to have access to a "yes" or "no" response through a trusted third party.

Complying with Regulatory Requirements

As you know, financial institutions are heavily regulated and actively supervised by the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of Currency, Office of Thrift Supervision, National Credit Union Administration, and the Securities and Exchange Commission. Regulators have stepped up their oversight on business continuity, information security, third party service providers, and critical infrastructure protection. Our industry is working consistently and diligently to comply with new regulations and ongoing examinations. In addition, BITS and other industry associations have developed and disseminated voluntary guidelines and best practices as part of a coordinated effort to strengthen all critical players in the sector.

Regardless of how well financial institutions respond to regulations, we simply cannot address these problems alone. Our partners in other critical industry sectors—particularly the telecommunications and software industries—must also do their fair share to ensure the soundness of our nation's critical infrastructure.

Recommendations

The Congress can help the financial services sector meet the challenges of a post 9/11 environment in a number of ways. We have developed these key recommendations for the Committee to consider:

1. Recognize that the financial sector is driven by its "trusted" reputation as well as regulatory requirements. Other industries do not have the same level of regulatory oversight, liability, or business incentives. However, we rely on other sectors because of our interdependencies. Responsibility and liability need to be shared.

2. Maintain rapid and reliable communication. Critical infrastructure industries and the public need to have an early understanding of the scope and cause as early as possible when a major event occurs. Diverse communication channels such as cell phones, wireless email devices, landline phones, and the Internet are necessary. Both diversity and redundancy are needed within critical infrastructures to assure backup systems are operable and continuity of services will be maintained.

3. Recognize the dependence of all critical infrastructures on software operating systems and the Internet. Given this dependence, the Congress should encourage providers of software to the financial services industry to accept responsibility for the role their products and services play in supporting the nation's critical infrastructure. In so doing, Congress should support measures that make producers of software more accountable for the quality of their products and provide incentives such as tax incentives, cyber-insurance, liability/safe harbor/tort reform, and certification programs that encourage implementation of more secure software. Congress also could provide protection from U.S. antitrust laws for critical infrastructure industry groups that agree on baseline security specifications for the software and hardware that they purchase.

4. Encourage regulatory agencies to review software vendors—similar to what the regulators currently do in examining third-party service providers—so that software vendors deliver safe and sound products to the financial services industry.

5. Encourage collaboration and coordination among other critical infrastructure sectors and government agencies to enhance the diversity and resiliency of the telecommunications infrastructure. For example, the government should ensure that critical telecommunications circuits are adequately protected and that redundancy and diversity in the telecommunications networks are assured.

6. Invest in the power grid because of its critical and cascading impact on other industries and other critical infrastructures. The power grid must be considered among the most vital of critical infrastructures and needs investment to make sure it works across the nation.

7. Establish improved coordination procedures across all critical infrastructures and with federal, state, and local government when events occur. Coordination in planning and response between the private sector and public emergency management is inadequate and/or inconsistent. For example, a virtual national command center for the private sector that links to the Homeland Security Operations Center would help to provide consistency.

8. Encourage law enforcement to prosecute cyber criminals and identity thieves, and publicize U.S. government efforts to do so. These efforts help to reassure the public and businesses that the Internet is a safe place and electronic commerce is an important part of the nation's economy.

On behalf of both BITS and The Financial Services Roundtable, thank you for the opportunity to testify before you today. I will now answer any questions.

Attachment A

Letter from BITS and The Financial Services Roundtable

THE FINANCIAL SERVICES ROUNTABLE

BITS

FINANCIAL SERVICES

ROUNTABLE

JULY 13, 2004

REPRESENTATIVE CHRISTOPHER COX,
Chairman, Select Committee on Homeland Security
2402 Rayburn House Office Building
Washington, DC 20515

REPRESENTATIVE JIM TURNER
Ranking Member, Select Committee on Homeland Security
330 Cannon House Office Building
Washington, DC 20515

REPRESENTATIVE MAC THORNBERRY
Chairman, Cybersecurity Subcommittee
2457 Rayburn House Office Building
Washington, DC 20515

REPRESENTATIVE ZOE LOFGREN
Ranking Member, Cybersecurity Subcommittee
102 Cannon House Office Building
Washington, D.C. 20515

RE: Cybersecurity Concerns

Dear Representatives Cox, Turner, Thornberry and Lofgren:

Thank you for the opportunity to discuss the concerns of financial institutions with regard to strengthening software security.

The Financial Services Roundtable (FSR) and BITS want to offer our support for the recommendation to elevate the position of cybersecurity director to the level of Assistant Secretary. We support this effort as a way to increase the administration's focus on cybersecurity concerns and address issues such as those outlined in the attached BITS/FSR Software Security Policy Statement. Furthermore, we believe that this elevation to Assistant Secretary will provide support for those areas identified by the National Strategy as requiring additional actions.

Finally, we would like to acknowledge the responsiveness of the National Communications System (NCS) to meeting the needs of the financial services industry. As such, we would like to ensure that moving the NCS into the Cybersecurity Division will not undermine the excellent work of the NCS.

Best regards,

STEVE BARTLETT
President, The Financial Services Roundtable.

CATHERINE A. ALLEN
Chief Executive Officer.

Enclosure: BITS/FSR Software Security Policy Statement

SOFTWARE SECURITY

Security is a fundamental building block for all financial services. It is also a regulatory requirement. The financial services industry relies upon software to operate complex systems and provide services, as well as to protect customer information.

Financial services companies comply with a host of legal and regulatory requirements to ensure the privacy and security of customer information. Recently, the prevalence of security risks, threats and viruses, combined with a lack of accountability for software vulnerabilities, has saddled financial institutions with significant risks and skyrocketing costs.

In early 2004, BITS surveyed its members to estimate the costs to financial institutions of addressing software security and patch-management problems. Based on the survey, BITS and Financial Services Roundtable members pay an estimated $400 million annually to deal with software security and patch management. Extrapolated to the entire financial services industry, these costs are approaching $1 billion annually.

The members of BITS and The Financial Services Roundtable believe:

- Because the financial services industry plays a central role in the nation's critical infrastructure and is dependent on the products and services of software providers, such providers of mission critical software to the financial services industry need to accept responsibility for the role their products and services play in supporting the nation's critical infrastructure and should exhibit and be held to a "higher duty of care" to satisfy their own critical infrastructure responsibilities.
- Software vendors should ensure their products are designed to include security as part of the development process using security-trained and security-certified developers on product development and lifecycle teams.
- Software vendors should ensure through testing that their products meet quality standards and that financial services security requirements are met *before* products are sold.
- Software providers should develop patch-management processes that minimize costs, complexity, downtime, and risk to user organizations. Software vendors should identify vulnerabilities as soon as possible and ensure that the patch is thoroughly tested.
- Software vendors should continue patch support for older, but still viable, versions of software.
- Collaboration and coordination among other critical infrastructure sectors and government agencies are essential to mitigate software security risks.

The members of BITS and The Financial Services Roundtable:

- Support measures that make producers of software more accountable for the quality of their products.
- Support incentives (e.g., tax incentives, cyber-insurance, liability/safe harbor/tort reform, certification programs) and other measures that encourage implementation of more secure software development processes and sustain long-term R&D efforts to support stronger security in software products.
- Seek protection from U.S. antitrust laws for critical infrastructure industry groups that agree on baseline security specifications for software and hardware that they purchase.
- Encourage regulatory agencies to explore supervisory tools to ensure that critical third-party service providers and software vendors deliver safe and sound products to the financial services industry.
- Support and incorporate, where possible, the BITS Product Security Criteria into security policies, and encourage technology vendors to test products to meet these criteria.
- Apply a risk-management approach to software security by assessing risks and applying appropriate tools and best practices to ensure the most secure deployment and application of software possible across the entire enterprise.
- Participate in and support efforts to strengthen the Financial Services Information Sharing and Analysis Center (FS/ISAC) in order to share vulnerability information on the products deployed by financial institutions.
- Educate policy makers on the significance of the risks posed to the financial services sector and other critical infrastructure industries and the need to take action to mitigate these risks.

BUSINESS REQUIREMENTS

FOR

SOFTWARE SECURITY AND PATCH MANAGEMENT

Members of BITS and The Financial Services Roundtable believe software vendors should take responsibility for the quality of their products. Especially when selling products to companies that are within critical infrastructure industries, certain minimum requirements should be met. Following are recommended critical infrastructure sector Business Requirements.

Provide a higher "duty of care" when selling to critical infrastructure industry companies.

To meet this higher duty of care, vendors should:

- Make security a fundamental component of software design.
- Support older versions of software (e.g., NT), particularly if existing programs are functional and not past the end of their estimated life cycle.
- Make upgrading easier, less cumbersome and less costly, and offer more support.
  - — Products should be less prone to failure and have an automated back-out feature.
  - — Components (including embedded components used in other products) should be clearly defined in order for the customer to assess the cascading effect of the upgrade or installation.
  - — Publish metrics on security of new and existing products.
  - — Expand coordination and establish better communication with individual clients and industry groups.
  - — Vendors should give customers an aggressive "patch playbook" which would provide clear guidance and explicit instructions for risk mitigation throughout the patch management process and especially in times of crisis.
  - — Vendors should offer critical infrastructure customers access to one-on-one, private, early vulnerability notice prior to notifying the general public, possibly by establishing "preferred" customer levels. (Some vendors offer financial institutions advanced notification if they agree to serve as a "beta" site, however, this is not practical as an industry-wide solution.)
- Provide better security-trained and security-certified developers on product teams.
- Establish Regional Centers of Excellence to service major financial institutions in their area. Centers would keep IT profiles for each institution in order to:
  - — Inform institutions of the likely effects of a new vulnerability on their specific IT environment.
  - — Continually advise institutions on how to best apply patches.
  - — Expedite patch installation by visiting the financial institution site.
  - — Make on site or remote consultation available when patches affect other applications.

Comply with security requirements before releasing software products.

Vendors should:

- Meet minimum security criteria, such as BITS software security criteria and/or the Common Criteria.
- Thoroughly test software products, taking into consideration that:
  - — Testing needs to address both quality assurance as well as functionality against known and unknown threats.
- Conduct code reviews.
  - —Whether conducted internally or outsourced, code reviews should involve tools or processes, such as code profilers and threat models, to ensure code integrity.

Improve the patch-management process to make it more secure and efficient and less costly to organizations.

Vendors should:

- Issue patch alerts as early as possible.
- Continue patch support for older software.
  - — Vendors should be clear about the level of support provided for each software version.
  - —Vendors are strongly encouraged to provide support for up to two versions of older software, i.e., the N–2 level.
- Provide automatic, user-controlled patch-management systems, such as uniform, reliable, and, possibly, industry-standard installers.

- Ensure all patches come with an automated back-out function and do not require reboots.
- Support clients who purchase third-party installer tools (until a standard is established).
- Thoroughly test patches before release.
  — Testing should include patch-to-patch testing to identify any cascade effects and in-depth compatibility testing for effects on networks and applications.
- Issue better patch and vulnerability technical publications. Publications should include more thorough analyses of the impact of vulnerabilities on unpatched systems as well as data on the environments and applications for which the patches were tested. Impact on other patches should also be addressed.
- Conduct independent security audits of the patch-development and deployment processes.
- Distribute a communication and mitigation plan, including how vulnerability/patch information will be relayed to the customer, for use in times of crisis.

Attachment B

BITS RESPONSE TO DHS' QUESTIONS ON CYBER SECURITY JANUARY 4, 2005

The National Cyber Security Division of DHS hosted a retreat at Wye River, Maryland on January 6–7, 2005 to assess private and public sector progress in meeting the goals and objectives of the Administration's National Strategy to Secure Cyberspace. DHS asked participants in advance of the meeting to answer three questions. BITS submitted the following answers to these questions.

Question 1: What are the top three initiatives your organization is currently involved in to advance cybersecurity (such as the goals articulated in the National Strategy to Secure Cyber Space)?

BITS is involved in numerous efforts to address cyber security and protect the Nation's critical infrastructure. **For 2005, BITS will focus on the following top three initiatives to advance cybersecurity: (1) urge major software vendors to address software security business requirements; (2) combat on-line fraud and identity theft; and (3) support efforts to develop meaningful software product certification programs.** In addition to the three initiatives outlined below, BITS also will continue to educate policy makers on cyber security risks and steps that can be taken to protect the Nation's critical infrastructure. (See appendix B for a summary of BITS' accomplishments in 2004.)

A. Urge major software vendors to address the BITS/FSR software security business requirements. In April 2004, BITS and The Financial Services Roundtable announced a joint policy statement calling on the software industry to improve the security of products and services it provides to financial services customers. The policy statement calls on software providers to accept responsibility for their role in supporting financial institutions and other critical infrastructure companies. BITS and the Roundtable support incentives (e.g., tax incentives, cyber-insurance, liability/safe harbor/tort reform, certification programs) and other measures that encourage implementation of more secure software development processes and sustain long-term research and development efforts to support stronger security in software products. (The BITS/FSR Software Security Business Requirements are attached to the April 2004 BITS/FSR Software Security Policy statement which is available at *http://www.bitsinfo.org/bitssoftsecuritypolicyapr04.pdf*) In addition, BITS is working with major software vendors to discuss business requirements. In June 2003, BITS announced it had successfully negotiated with Microsoft to provide additional support to BITS member companies for Windows NT. We have provided Microsoft and other software and hardware companies with the Software Security Business Requirements. BITS members agree that these requirements are critical to the soundness of systems used in the financial services industry. BITS also is working with or has plans in early 2005 to work with Cisco, IBM and RedHat on software security issues.

B. Combat on-line fraud and identity theft and explore appropriate authentication strategies. BITS is involved in supporting the pilot of the BITS/FSR Identity Theft Assistance Center (ITAC), developing the BITS Phishing Prevention and Investigation Network, and focusing on authentication practices and strategies.

The ITAC is a one-year pilot program intended to help victims of identity theft by streamlining the recovery process and enabling law enforcement to identify and prosecute perpetrators of this crime. ITAC is an initiative of The Financial Services Roundtable and BITS, which represent 100 of the largest integrated financial services companies. Fifty BITS and Roundtable Members are participating and funding

the ITAC pilot program as a commitment to their customers and maintain trust in the Nation's financial services system. The ITAC's services are free-of-charge to customers and made available based on referrals to the ITAC by one of the 50 members of the ITAC pilot program. BITS has also published several business practices guidelines and white papers on various aspects of identity theft and fraud reduction strategies.

The BITS Phishing Prevention and Investigation Network has three primary purposes. First, the Network helps financial institutions shut down online scams. Second, it aids in investigations of scam perpetrators by providing law enforcement with trend data. Law enforcement agencies can use the data to build cases and stop scamming operations. Finally, the BITS Network facilitates communication among fraud specialists at financial institutions, law enforcement agencies and service providers, resulting in a "united front" for combating online scams. Financial institutions can also use the BITS Network to share information about online scams. Through its searchable database, fraud professionals at BITS member institutions learn from other institutions' phishing incidents and responses. The database provides quick access to contacts at law enforcement agencies, foreign governmental agencies, and ISP administrators. Founded under the auspices of the BITS eScams Subcommittee of the BITS Internet Fraud Working Group, the Network is hosted by the Financial Services Information Sharing and Analysis Center (FS/ISAC). Resources to develop the Network were contributed by Microsoft Corporation and RDA Corporation.

On March 8, 2005, BITS will host a Forum entitled "A Strategic Look at Authentication" in Washington, DC. Authentication issues have emerged in a number of BITS' working groups. This strategic Forum will focus on the following issues: business issues that drive the need for authentication; business challenges to implementation; public policy implications; and emerging technologies in the authentication area.

C. Support efforts to develop meaningful software product certification programs. The BITS Product Certification Program (BPCP) is an important part of our work to address software security. The BPCP provides product testing by unbiased and professional facilities against baseline security criteria established by the financial services industry. A product certification, the *BITS Tested Mark,* is awarded to those products that meet the defined criteria. An option is available for technology providers to meet the product certification requirements via the internationally recognized Common Criteria certification schema. BITS has initiated discussions with DHS to support efforts to enhance product certification programs, including the Common Criteria program run by the National Security Agency (NSA) and National Institutes of Technology and Standards (NIST). DHS has expressed support for broad-based, not sector specific, certification programs. Moreover, DHS wants "buy in" from the broader user community. Consequently, BITS has been in discussions with The Business Roundtable, NIST, and the Cyber Security Industry Alliance (CSIA) to develop a joint proposal.

Question 2 & 3: Aside from funding, what can the government (if appropriate, specify which agency(ies)) do to help advance the cybersecurity agenda/priority(ies)/initiative(s) of your organization? What else should government and the private sector be doing to help facilitate enhanced cybersecurity?

Our Nation's economic and national security relies on the security of information technology (IT). This security depends on the reliability, recoverability, continuity, and maintenance of information systems. The issue of secure information technology has a direct and profound impact on both the government and private sectors, and includes the Nation's critical infrastructure. The security and reliability of information systems are increasingly linked to consumer and investor confidence. Financial institutions (and others that make up the "user" community) are demanding greater accountability for the security of IT products and services. The federal government can play an important role in protecting the Nation's IT assets. The following are steps the U.S. government can and should take to secure information technology.

- **Strengthen the Information Sharing and Analysis Centers (ISACs) by providing complete and adequate federal funding.** Information sharing and trend analysis within a sector is essential to protecting information security and responding to events. The ISACs are a good vehicle for such sharing, but they require additional resources.
- **Encourage sharing of essential information among industry ISACs.** Threats to cyber security will reach some sectors before others—oftentimes resulting in simultaneous or cascading effects. Mandatory sharing among the ISACs will provide valuable advance notice to sectors not immediately threatened.

• **Utilize the ISACs to inform critical infrastructures of cyber threats discovered through national intelligence and law enforcement.** As a primary target of cyber attacks, the government expends substantial resources to protect, detect and respond to attacks. The information gathered by the government regarding present, imminent, or gathering threats should be shared with sectors that are widely understood to be critical to the security of the country. ISACs represent a centralized way of quickly disseminating important security information.

• **Create an emergency communication system in the event of a massive cyber attack.** Such an attack could potentially cripple many of the primary communication channels. To allow maximum efficiency of information dissemination to key individuals in such an event, a thorough and systematic plan should be in place. The financial services industry relies on the BITS/FSR Crisis Management Process and Manual of Procedures, including the BITS/FSR Crisis Communicator.

• **Create and promote security standards for technology products which address the Common Criteria certification concerns noted by the National Cyber Security Partnership (NCSP).** These concerns include:

- Cost and delay of the certification process
- Need to make certification applicable to the needs of both government and industry
- Uniform tying of federal procurement policies to the certification system

In the alternative to repairing the Common Criteria, a new system should be developed that would address from the beginning the limitations of the Common Criteria. DHS has expressed interest in such a certification program if it is not sector specific. The BITS Product Certification Program may well be able to serve as a model for such a certification program.

• **Increase staffing, funding, and prominence of cyber security in the DHS.** Cyber security is a unique threat to national security. As such, it should be elevated in importance at DHS.

• **Create a more senior level policy level position within DHS to address cyber security issues and concerns.**

• **Provide tax or other incentives for achieving higher levels of Common Criteria certification.** Presently, Common Criteria certification is the primary uniform means of evaluating the security of software and hardware. Incremented incentives, based upon the level of certification achieved, would help to compensate companies for the time and cost of certification. This should encourage more certification and increase the overall security of hardware and software.

• **Provide tax or other incentives for certification of revised or updated versions of previously certified software.** Under Common Criteria, certification of updated versions is costly and time consuming. Incentives are necessary to ensure that all software is tested for security and not a single build or version of a product.

• **Require software providers to immediately notify ISACs of newly discovered cyber threats and to provide updated information on such threats until an effective patch is provided.** Regulatory controls may be necessary to prevent the wider broadcast of such information, but it is vital that the critical infrastructure receive immediate notice of serious vulnerabilities. Regulatory action will also be necessary to police software provider compliance with such an information sharing requirement.

• **Establish requirements which improve the patch-management process to make it more secure and efficient and less costly to organizations that use software.**

• **Fund joint FTC/DHS consumer cyber security awareness campaign.** The FTC should focus its efforts on building consumer awareness, and DHS should coordinate more detailed technical education regarding specific serious threats. In addition, government employees should be trained in proper cyber safety measures.

• **Train government employees on proper cyber security measures.**

• **Provide tax or other incentives for industry cyber security awareness campaigns.** Because security should not be grounds for competitive advantage, cyber security awareness campaigns undertaken on an industry-wide basis should be encouraged.

• **Educate corporate executives and officers regarding their duties under Sarbanes-Oxley, GLBA, and HIPAA as relates to cyber security.**

- **Require high levels of cyber security in software purchased by the government through procurement procedures.** Extend such requirements to software used by government contractors, subcontractors, and suppliers.
- **Provide NIST with adequate resources to develop minimum cyber security requirements for government procurement.** NIST should include software developers and other stakeholders in the standard creation process.
- **Assign to the Commerce Department or another appropriate agency the responsibility of tracking and reporting such costs and the impact on the economy.** Measuring and making transparent these costs will aid law makers and regulators as they assign resources to cyber security programs.
- **Fund research and development of more secure software development practices, testing and certification programs.**
- **Facilitate collaboration with the users and suppliers of information technology to develop standards for safe practices.**
- **Enhance DHS, NSF, and DARPA cyber security R&D funding.**
- **Carefully manage long and short term R&D to avoid duplication.**
- **Establish a mechanism to share educational training and curriculum.**
- **Encourage law enforcement to enforce, investigate and prosecute cyber crimes here and abroad.**
- **Ratify the Council of Europe's Convention on Cybercrime.**
- **Enhance criminal penalties for cyber crimes.**
- **Make cyber crimes and identity theft enforcement a priority among law enforcement agencies.**
- **Encourage better coordination among law enforcement agencies in order to detect trends, share information and identify and prosecute offenders.**

Mr. LUNGREN. I think the chief clerk wants to make sure that we hear Mr. Silva. This is high-tech right here.

The Chair now recognizes Mr. Ken Silva, chairman of the board of directors of the Internet Security Alliance, to testify. Thank you for appearing.

STATEMENT OF KEN SILVA, CHAIRMAN OF THE BOARD OF DIRECTORS, INTERNET SECURITY ALLIANCE

Mr. SILVA. Good morning, Mr. Chairman.

I am Ken Silva. I am the chief security officer and vice president for infrastructure security of VeriSign, Incorporated. I am also chairman of the board for the Internet Security Alliance, on whose behalf I am here today. With the Chairman's permission, I ask that my entire statement be inserted into the record.

Before I detail what is in H.R. 285 that the IS Alliance finds promising, let me tell you a little bit about ISA and one of its members companies, VeriSign. ISA was established in April of 2001 as a trade association comprising over 200 member companies spanning four continents. ISA member companies represent a wide diversity of economic sectors representing the vendors and users of the technology network, and the ISA focuses exclusively on information security issues. Among IS Alliance's core beliefs are, first, because we are the stewards of the Internet's physical assets, it is the private sector's responsibility to aggressively secure them.

Second, more needs to be done by both government and industry to provide adequate information security. This means security not only securing the physical and logical elements of the network, but also securing the highly valuable electronic cargo running over the network.

Third, a great deal can be accomplished simply with enhanced technology and greater awareness and training of individuals, from the top corporate executives down to the solitary PC user.

Fourth, while technology, education and information sharing are critical to cybersecurity, they must be supported by research, aggressive global intelligence gathering, information sharing, and vigorous law enforcement efforts against those who attack the network.

Lastly, new and creative structures and incentives need to evolve to ensure adequate and ongoing information security. VeriSign, as one of the member companies of the Internet Security Alliance, is in a unique position to preserve and protect the Internet's infrastructure, at least part of it, in our role as steward for the dot.com and dot.net top-level domains of the Internet and also 2 of the 13 root servers.

I am pleased to have the opportunity to speak in support of H.R. 285, the Department of Homeland Security Cybersecurity Enhancement Act of 2005. I would like to make three overarching points about this legislation.

First, both the public and private sectors need to become more proactive with respect to cybersecurity. The FBI declares cybercrime to be our Nation's fastest-growing crime. According to the CERT, there has been an increase of nearly 4,000 percent in computer crimes since 1997. We also know from reliable intelligence that has been reported that terrorist groups are not only using cybercrime to fund their activities, but studying how to use the information and attacks to undermine our critical infrastructures.

Second, the administrative changes in management tasking set out in H.R. 285 must be supported by an adequate level of funding to permit the Department to carry out critical mandates of this bill. In particular, increased funding for cybersecurity research is one critical area not specifically mentioned in this legislation. The Internet's basic protocols are nearly 30 years old, and at the time of their creation, they didn't contemplate the security or scale issues we face today.

Third, sufficient real authority and trust must be invested in the person who heads up the cybersecurity organization. Without this stature and trust, the elevation of the organization to an office and the bestowing of an assistant secretary title will have little benefit.

Mr. Chairman, there is no shame in pointing out what we all know to be true. Our economic and national security depends on this job being done right. Cybersecurity means the protection of physical and logical assets of a complex distributed network. Cybersecurity means protection of the economic and national security activity carried on that infrastructure.

These infrastructure assets support activity that in the commercial area alone account for about $3 trillion daily. According to the Federal—excuse me, this is according to the Federal Reserve Board. That is $130 billion an hour that depends on there being a safe, reliable and available Internet. An infrastructure of such great importance to America's economic and national security demands leadership that is trusted, visible and effective.

In summary, Mr. Chairman, the challenge of America and the rest of the Internet-dependent world, security organizations like DHS, is threefold. First, DHS and other government cyberagencies

need to understand the architecture of the network today and to recognize its ever-growing diversity and complexity.

Second, cybersecurity agencies need to collaborate with the industries that operate most of these network assets and exchange and understand the information exchanged with industry, including employing the best engineering talent available.

Lastly, the cybersecurity agencies here and around the world must be organized and cooperate to respond to threats and attacks against our cyberinfrastructure rapidly and effectively.

Mr. Chairman, this H.R. 285 moves the Department of Homeland Security in the direction of addressing these three challenges. It is especially helpful simply because it applies more attention to cybersecurity.

IS Alliance members want to work with the committee and the Department to ensure that good intentions expressed in this document become a reality that strengthens America's ability to prevent attacks against our networks and to make them strong enough to withstand any attacks that do come our way.

Thank you, Mr. Chairman.

Mr. LUNGREN. Thank you very much, Mr. Silva.

[The statement of Mr. Silva follows:]

PREPARED STATEMENT OF KEN SILVA

Good morning Mr. Chairman. I am Ken Silva. I am the Chief Security Officer and Vice President for Infrastructure Security of VeriSign, Incorporated. I have the privilege of being the Chairman of the Board of the Internet Security Alliance (ISAlliance), on whose behalf I am here today

Before I detail what it is in H.R. 285 that the IS Alliance finds promising, let me tell you a bit more about both the IS Alliance and VeriSign.

Established in April 2001 as collaboration between Carnegie Mellon University and the Electronic Industries Alliance, the IS Alliance is a trade association comprising over 200 member companies spanning four continents. IS Alliance member companies represent a wide diversity of economic sectors including banking, insurance, entertainment, manufacturing, IT, telecommunications, security, and consumer products.

The IS Alliance programs focus exclusively on information security issues. We provide our member companies with a full suite of services including: information sharing, best practice, standard, and certification development, updated risk management tools, model contracts to integrate information technology with legal compliance requirements, and market incentives to motivate an ever-expanding perimeter of security.

Among the IS Alliance's core beliefs are:

First, because the Internet is primarily owned and operated by private organizations, it is the private sector's responsibility to aggressively secure the Internet.

Second, not enough is currently being done by either government or industry to provide adequate information security. This means security not only of the physical and logical elements of the network—but also security of the highly valuable electronic cargo running over the network. Third, a great deal can be accomplished simply with enhanced technology and greater awareness and training of individuals—from the top corporate executives down to the solitary PC users.

Fourth, while technology, education, and information sharing are critical, they are insufficient to maintain appropriate cybersecurity and respond to an ever-changing technological environment. Research, aggressive global intelligence gathering, information sharing, and vigorous law enforcement efforts against those who attack our networks are also essential.

Fifth, new and creative structures and incentives may need to evolve to assure adequate and ongoing information security. While government is a critical partner, industry must shoulder a substantial responsibility and demonstrate leadership in this field if we are to eventually succeed.

As Chairman of ISAlliance's Board, one of my roles is to carry these messages not only to government, but also to potential new members of the ISAlliance. When VeriSign helped found the ISAlliance four years ago, there were fewer than a dozen

members. But the ISAlliance's key points resonate with ANY organization that uses the information superhighway to conduct its affairs?whether commercial business, academic institution, NGOs, or government. Thus, it is not surprising that, since its inception, the ISAlliance has grown by nearly twenty-fold.

Certainly, my own company, VeriSign takes these principles seriously. VeriSign is a microcosm of the diverse "e" activities on the Internet, of the convergence of the traditional "copper" networks with computer driven digital networks, soon to become the "NGNs" or Next Generation Networks. Commerce, education, government, and recreation all are enabled by the infrastructures and services we and our colleague companies support. VeriSign, the company I am privileged to serve as Chief Security Officer, was founded 10 years ago in Mountain View, California. VeriSign operates the Internet infrastructure systems that manage .com and .net, handling over 14-billion Web and email look-ups every day. We run one of the largest telecom signaling networks in the world, enabling services such as cellular roaming, text messaging, caller ID, and multimedia messaging. We provide managed security services, security consulting, strong authentication solutions, and commerce, email, and anti-phishing security services to over 3,000 enterprises and 400,000 Web sites worldwide. And, in North America alone, we handle over 30 percent of all e-commerce transactions, securely processing $100 million in daily sales.

Of these activities, the one that places us in a very unique position to observe, and to protect the Internet's infrastructure is our role as steward of the .COM and .NET top level domains of the Internet, and of two of the Internet's 13 global root servers. These are the Internet's electronic "directory" The services VeriSign provides over many hundreds of millions of dollars worth of servers, storage and other infrastructure hardware enables the half *trillion* daily Internet address lookups generated by all of your web browsing and emails to actually reach their intended destinations. Consequently as the manager of several 24x7 watch centers where our engineering staff observe as these 500 billion daily requests circle the globe, we see when elements of the infrastructure are attacked, impaired, taken off the air for maintenance, or otherwise have their status or performance altered. Because we observe and record this, VeriSign is capable of, and often involved in the identification of the nature, severity, duration, type, and sometimes even source of attacks against the Internet. Our experience in doing this for over a decade, I believe makes VeriSign uniquely interested in how the government architects its companion cybersecurity services.

I am pleased to have the opportunity to speak in support of H.R. 285, the Department of Homeland Security Cybersecurity Enhancement Act of 2005; I would like to make three overarching points about the legislation:

First, both the public and private sectors need to become more pro-active with respect to cybersecurity.

A smattering of statistics can briefly outline the growing nature of the growing cyber security problem. According to Carnegie-Mellon University's CERT, there has been an increase of nearly 4000 percent in computer crime since 1997. The FBI declares Cybercrime to be our nation's fastest growing crimes. One FTC estimate puts the number of Americans who have experienced identity theft at nearly 20 million in the past 2 years, suggesting the link between Cybercrime and identity theft is not merely coincidental. CRS reported last year that the economic loss to companies suffering cyber attacks can be as much as 5 percent of stock price. Furthermore, the OECD reports that as many as 1 in 10 e-mails are viruses and that every virus launched this year has a zombie network backdoor or Trojan (RAT). Globally they estimate 30 percent of all users, which would mean more than 200 million PCs worldwide, are controlled by RATs.

Perhaps most ominously, we know from reliable intelligence that terrorist groups are not only using Cybercrime to fund their activities, but are studying how to use information attacks to undermine our critical infrastructures.

Second, the administrative changes and management taskings set out in H.R. 285 must be supported by an adequate level of funding to permit the Department to carry out the critical mandates of this bill.

In particular, cybersecurity research is one area of critical financial need NOT specifically mentioned in the legislation. The basic protocols the Internet is based on are nearly 30 years old; they did not contemplate the security or scale issues we face today and will continue to face in the future. Increasing Federal funding for cybersecurity research and development was recently cited by the President's Information Technology Advisory Committee, (the "PITAC"). After studying the U.S. technology infrastructure for nearly a year, PITAC noted in its report entitled ?Cyber Security: A Crisis of Prioritization? that ?most support is given to short-term, defense-oriented research, but that little is given to research that would address larger security vulnerabilities." The IS Alliance fully agrees. Substantial fund-

ing needs to be provided for basic research in cybersecurity. Industry, itself, can not sustain the level of research investment that is required. The US government must increase its investment.

Third, sufficient REAL authority and trust need to be invested in the person who heads up the Cybersecurity organization within the Department. Without this stature and trust, the elevation of the organization to an ?Office? and the bestowing of an Assistant Secretary title will have little benefit. Mr. Chairman, there should be no shame in pointing out what we all know to be true: our economic and national security depends on this job being done right.

"Cybersecurity" means the protection of the physical and logical assets of a complex distributed network comprised of long-haul fiber, large data switching centers, massive electronic storage farms, and other physical assets worth hundreds of billions of dollar; the software programs, engineering protocols, and human capital and expertise which underlie it all are equally valuable. And cybersecurity means protection of the activity—economic and national security—carried on that infrastructure. All of these infrastructure assets combine to support activity that, in the commercial area alone, account for about $3 trillion dollars daily, according to the Federal Reserve Board. That's $130 billion per hour that depends on a safe, reliable, and available Internet. An infrastructure of such great importance to America's economic and national security demands leadership that is trusted, visible, and effective.

Several provisions of H.R. 285 are of special note:

First, the final section does us all the important service of attempting to define—and to BROADLY *"define—cybersecurity"*, to encompass all of the diverse legacy, present and emerging networked electronic communications tools and systems.

Second, the bill's repeated emphasis *on collaboration between the Department and the private sector*—in each present and proposed NCSO operational area, as well as across government—reflects a wise understanding of the dynamic nature of the cyber infrastructure, and the diverse interests in and out of government which must cooperate to assure the networks' security and stability. I will address some specifics, as well as IS Alliance's incentives programs, later in my testimony.

Third, in a related area, language in Section 2 (d) *directs the consolidation into the NCSO of the existing National Communications System (NCS) and its related NCC industry watch center,* which for two decades has provided industry-based alert, warning, and analysis regarding attacks against the traditional telephone networks. These existing important watch functions support critical national security and emergency preparedness communications; their consolidation will bring Departmental practice more inline with emerging technological realities. If done with appropriate care and recognition of the valuable, unique role the NCC has played in supporting NS/EP communications for two decades, consolidation could also make the function stronger and better able to protect these converging assets.

Fourth, the ISAlliance strongly supports *voluntary cybersecurity best practices* highlighted in section 5(A). We believe that market-driven cyber security is the appropriate model to compel positive cybersecurity improvements within the nation's cyber critical infrastructure. Towards this end, the insurance industry, among others, have made great strides and continue to advance the state-of-the-art among market-driven cybersecurity best practices.

COMMENTS on SPECIFIC PROVISIONS

Developing new tools to address cyber threats depends on real public-private cooperation. H.R. 285 provides the Department with significant improvements that the ISAlliance believes may help achieve better organization, more cooperation, and greater effectiveness in its collaborations with the industrial, private-sector custodians of the cyber infrastructure, in its cooperation with other agencies of government at the Federal, sub-Federal and international levels, and in its development of new tools to combat cyber threats.

With its focus on government-industry cooperation and cross-governmental cooperation, this bill correctly identifies the two centers of gravity for successfully meeting the cybersecurity challenge. Current programs must continue, which address:

- analysis of threat information;
- detection and warning of attacks against the cyber infrastructure;
- restoration of service after attacks;
- reducing vulnerabilities in exiting network infrastructure, including assessments and risk mitigation programs;
- awareness, education, and training programs on cybersecurity across both the public and private sectors;

- coordination of cybersecurity (as directed by HSPD–7 and the Homeland Security Act) across Federal agencies, and between Federal and sub—federal jurisdictions; and
- international cybersecurity cooperation.

All of these are essential functions. Even in our custodial role for many of the infrastructures that support the $10 trillion U.S."eConomy", few would assert that private industry can, or even SHOULD, manage these functions. They are PUBLIC functions, properly performed by government, but in cooperative collaboration—persistent and polite collaboration between government and industry. I want to note here, Mr. Chairman, that we realize the challenges for DHS/NCSD are far, far easier said than done. Everyone working at the Department, including those in the infrastructure protection and cybersecurity divisions, deserves our sincerest gratitude. I want to personally thank my colleague on the panel today Mr. Yoran, as well as his predecessors, Mr. Clark & Mr. Simmons, as well as his successor Acting Director Purdy. And Mr. Liscouski who oversaw the entire infrastructure division; they all worked, or are working, as hard as they can at an imposing task.

That said however, it is a task that must be completed, no matter how difficult And IS Alliance is not unmindful of cost. But a national cybersecurity awareness and training program as provided by subsection (1) (C), a government cybersecurity program to coordinate and consult with Federal, State, and local governments to enhance their cybersecurity programs as provided by subsection (1) (D), and a national security and international cybersecurity cooperation program as provided by subsection (1)(E) are all important and welcome improvements to the nation's overall cybersecurity posture. Absent adequate funding however, the long-term effectiveness of these critical cybersecurity programs will be uncertain.

Unfortunately, and despite great effort to date, the track-record of the Department and NCSD in achieving even an effective *dialogue* on how to conduct these essential activities has been spotty and even disappointing.

The provisions of Section 2 of H.R. 285 that direct these specific functions may—hopefully, WILL—jumpstart the collaborations that will rapidly make these programs a reality. America cannot fail in doing these things; a cyber Pearl Harbor is not just a catch phrase, but very much a potential reality. The Department's own "Red Cell" exercises, including a notable one published last September, clearly forecasts "blended" terror attacks against the physical and logical assets of our information networks and institutions that depend on them. Such unavoidably attractive targets have the potential to disrupt economic, social, and government activities at all levels. Improved cyber-resiliency—established in part through effective public-private cooperation such as spelled out in Section 2 of H.R. 285—is one important step in reducing that threat.

Similarly, *cross-agency collaborations* within Department components—and with other security and anti-terrorism components of government—is not merely common sense, they are essential. In VeriSign's business, we have had opportunities from time to time to try to "go it alone" and reap the innovator's premium from the marketplace, or to cooperate with competitors on standards and accessible platforms that grow markets and increase business opportunities for all participants. I can tell you that cooperation and the "rising tide raises all boats" approach is preferable to being the single-handed sailor. In cybersecurity, the expertise of many different agencies—Treasury on financial crimes, or Justice on international frauds—being brought to bear just seems compelling.

Several other provisions of the bill have been long-standing areas of interest to the ISAlliance:

The *information sharing* provision of HR 285 refers back to Section 214 of the Homeland Security Act; the Department's "Protected Critical Infrastructure Information" program attempting to implement this Congressional mandate is long overdue for reexamination. The "PCII" program, though perhaps well meaning has, rather than encouraging information sharing between industry and the Department, chilled the flow of information. The implementing regulations represent a complex bureaucratic structure that seems more intent on keeping Federal employees from accidentally mishandling information, and thus facing prosecution, rather than encouraging a timely flow of attack and threat information from network custodians to the Department. VeriSign and some of our ISAlliance partners who are members of the IT–ISAC helped draft the original Section 214 of the Homeland Security Act. We are anxious to see it work in a manner consistent with its original Congressional intent and enable information flow that will help respond to attacks, mitigate the damage and, above all, prevent a recurrence.

And, as mentioned earlier, *the proposal to merge the watch functions of the NCS into NCSO,* and create a single, industry-supported watch effort that covers traditional and IP-based assets is clearly a beneficial way to manage the monitoring of

network exploits. However, cyber-security is not the sole mission of the National Communications System. Executive Order (EO) 12472 assigns the NCS with support for critical communications of the President and government including, the National Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget. The NCS was established by EO 12472 as a Federal interagency group assigned national security and emergency preparedness (NS/EP) telecommunications responsibilities throughout the full spectrum of emergencies—disaster and warfare as well as cyber attacks. These responsibilities include planning for, developing, and implementing enhancements to the national telecommunications infrastructure to achieve improvements in survivability, interoperability, and operational effectiveness under all conditions and seeking greater effectiveness in managing and using national telecommunication resources to support the Government during any emergency. While this mission does cover the spectrum of cyber-security issues, there is more to the legacy role of the NCS that must not be forgotten or overlooked and from which the NCSO can learn as these functions move forward together.

A key issue is missing from HR. 285, however. Funding for *cybersecurity research and development* is essential. The Director of the U.K.'s equivalent agency, the NISCC, observed recently that the U.K. alone last year spent 3 times as much on cyber R&D in 2004 as the $68 million spent by the Department and the National Academy's "cyber trust" programs to fund private sector cyber R&D. The United States should not be taking a second place position in the funding of cybersecurity research. While we are benefited by the many investments being made by intelligence and defense agencies that do not appear on such comparative scorecards, R&D to support improved security for the majority privately-held network assets must continue and must grow. In a tech industry where 2–3 percent is not an unusual R&D budget, the FY 2004 $68 million number is an amount you would expect *one $2 billion cyber company to spend on R&D, not the entire government* of the country that invented the technology.

We are increasingly seeing the solutions for improved security originating from research outside the United States, with outside investment and ownership in the solutions. Unless the U.S. commits to self-defense, funding the research locally at our universities that will produce solutions to secure our nation's economic infrastructure, we run the risk of having our security developed and managed by others than Americans—and that could be a fragile policy both economically and from the perspective of homeland security. We must figure out a way to invest more to match the clever advances being made by the terrorists who WILL attack these networks.

Finally, let me cite three examples of marketplace incentives that IS Alliance believe promote improved cybersecurity investment by industry: The ISAlliance, together with AIG, have agreed on a program wherein if member companies comply with our published best practices they will be eligible to receive up to 15 percent off their cyber insurance premiums. Visa, another ISAlliance member company, has developed its KISP program which again uses market entry, in this case the ability of commercial vendors to use the Visa card, as a motivator to adopt cybersecurity best practices. And the IS Alliance has recently launched its Wholesale Membership Program which allows small companies access to IS Alliance services at virtually no cost, provided their trade associations also comply with IS Alliance criteria.

There is also a role for the government to play in promoting industry cyber security; government should be a critical partner if incentive programs will have their maximum impact. Examples of critical incentive programs include the need to motivate and enhance the insurance industry participation in offering insurance for cyber-security risks, where AIG has been a leader, and the creation of private sector certification programs such as those provided by Visa in its Digital Dozen program. These and several other government incentive programs were highlighted last year in the report of the Corporate Information Security Working Group on Incentives which we commend to the Committee for its consideration.

In summary. Mr. Chairman, the challenge of America's—and the rest of the Internet-dependant world's security organizations—like the Department's is threefold:

First, DHS and other government cyber agencies need to *understand the architecture* of the network today and to recognize its ever-growing diversity and complexity;

Second, cybersecurity agencies need to *collaborate with the industries* that operate most of these network assets *and exchange and understand the information exchanged with industry* (including employing the best engineering talent available); and

Third, the cybersecurity agencies here and around the world need to *cooperate to respond to threats and attacks against our cyber infrastructure rapidly and effectively.*

Mr. Chairman, H.R. 285 moves the Department of Homeland Security in the direction of addressing these three challenges. It is especially helpful simply because it applies more attention to cyber security. ISAlliance members want to work with the Committee and the Department to assure that the good intentions expressed in this document become a reality that strengthens America's ability to prevent attacks against our networks and to make them strong enough to withstand any attacks that do come our way.

I appreciate the opportunity to bring our views before you today, and I am happy take any questions you may have.

Mr. LUNGREN. I thank all of you for your testimony. I would just like to ask a question of all of you, and that is it is premised on the fact that this hearing, while it is a hearing on a particular bill, is actually part of oversight in a sense. If we didn't think we needed a bill like this, we wouldn't be doing it for a position there.

So I would ask this, and I would just go down right to left, starting with Mr. Silva, and asking each of you, do you believe there is a sense of urgency to pass this bill so that it prods DHS to do what everyone seems to suggest we want DHS to be doing? Mr. Silva?

Mr. SILVA. Well, Mr. Chairman, I think that the sooner we start, if you will, getting on the ball with the cybersecurity issues, I think the better. Decisions around this have sort of floundered for long enough. The longer we wait, the longer this is going to linger as an issue and potentially lose interest. I think the sooner you could get this passed, I think it will express to the Department how urgent you feel this issue is. With our support, I think we will also reinforce that as well.

Mr. LUNGREN. Ms. Allen.

Ms. ALLEN. Yes. I do think there is a sense of urgency, first of all because of the escalation of attacks that are occurring; secondly, because we need leadership from the government; and, thirdly, I think, as said before, we have the potential of having a digital Pearl Harbor, and we want to avoid that.

Mr. LUNGREN. Mr. Kurtz. Everybody trying to share a computer monitor.

Mr. KURTZ. Yes. Simply stated, I think it is urgent that we seek passage of this. It has been 2 years since the National Strategy was issued. We have a crisis of organization and prioritization at DHS with regard to cybersecurity, and it would be nice if we could do this and not have to learn the hard way.

Having an assistant secretary will help develop those programs and plans and the communications issues in order for us, when we have an eventual attack, work out of it more cleanly than we are in a position now.

Mr. LUNGREN. Thank you.

Mr. Miller.

Mr. MILLER. Yes.

Mr. LUNGREN. Thank you.

Mr. Yoran.

Mr. YORAN. I am a cybersecurity strategist and operator. Just to point out the obvious, I am not particularly well versed in legislative process or motive. All of the fundamental concepts represented in this bill are well informed and constructive, and should be dealt with with the sense of urgency that they deserve.

Mr. LUNGREN. Well, let me ask you this. From your testimony, it doesn't sound to me like you think that it is right now receiving, that is the issue of cybersecurity, the kind of urgency, the kind of priority that is necessary. Would that be a correct characterization of your feeling?

Mr. YORAN. I would say that the threat against our Nation and our Nation's vulnerability to cyberattacks is increasing at a rate that is faster than the problem is being dealt with.

Mr. LUNGREN. Let me ask you this then, Mr. Yoran. If I were to ask you what the top three priorities would be, if we were to establish an Assistant Secretary of Cybersecurity, what would you say they would be; the most important priorities that we need right now to address from the standpoint of DHS, and, if this law passes, within the personification of this person as Assistant Secretary For Cybersecurity?

Mr. YORAN. Mr. Chairman, I believe that the single top priority for an assistant secretary, should one be created, would be to refine the Department's mission statement around the area of cybersecurity to go beyond the National Strategy and get to more specificity around what activities are under way within the Department, and also to point government counterparts as well as private sector counterparts to other components of the Federal Government which are playing an active role in our Nation's defense from cybersecurity threats. So that single top priority would be to refine the mission statement.

The second would be to integrate cybersecurity activities and priorities into and across all of the various programs of the Department of Homeland Security and across the Federal Government. So to the extent that cybersecurity and physical security risks have not been fully integrated and fully brought to the table to address vulnerabilities which may exist, I think that would be a top—a second priority for an assistant secretary.

The third would be in the area of resource allocation, once the mission definition has been refined; once more active participation has been integrated into various protection programs of the Department and across the Federal Government, to look at the resource allocation challenges and determine if the resources are sufficient for dealing with the refined mission and requirements.

Mr. LUNGREN. Thank you. My 5 minutes are up.

So Ms. Sanchez is recognized for 5 minutes of questions.

Ms. SANCHEZ. Thank you, Mr. Chairman, and thank you all for testifying once again.

I actually think that the whole arena of cybersecurity is so large and so vast and with so many things being so interconnected that it is just an incredibly overwhelming job. I represent Newport Beach, Santa Ana, Irvine area in Orange County, which, you know, is one of the top places for white-collar crime, most of it involving either telephone or computer. So it is just so overwhelming when my law enforcement officials tell me about all the scams that go on and the way that people get taken.

My question is about the identity theft that is going on in, like, for example, the ChoicePoint situation that we recently had. What do you think that a new Assistant Secretary of Cybersecurity should do or can begin to do to address some of these just large

databases that exist that can be either broken into or that you can pay $9.95 and find out everything you ever wanted to know about Loretta Sanchez, including her Social Security number, bank account and name of her kitty cat, et cetera? What are we going to do about that? Do you have any suggestions? I think that is just one of the scariest things that I see out there on the horizon for us. Any of you have any ideas on that?

Mr. MILLER. I think, Congresswoman, you have addressed a critical point. I think this is an example, again, where the assistant secretary position would make a difference, because what you are in need of is partnership between government and industry; having an assistant secretary there to work with the Treasury Department, with organizations like Ms. Allen's organization and others in the financial services industry and others to come up with an aggressive process that protects these data better, protects the citizens and the consumers whose data are at risk without harming electronic commerce, without making electronic transactions impossible to actually conduct.

Having someone at the assistant secretary level could convene a meeting along with his level, along with his or her colleagues and the other relevant agencies, as well as the Federal Trade Commission and Department of Treasury. But again, it is very hard to do that. It is very hard to have someone who is the head of the division to have internal clout to bring all the parties together and/or, frankly, to bring all the members of the industry together. So by passing this legislation that has been crafted by Congresswoman Lofgren and Mr. Thornberry, then you get the kind of clout you need to make these partnerships happen.

Ms. SANCHEZ. Thank you.

Anybody else on that?

Mr. KURTZ. I will expand briefly on what Harris has described. I think a lot of this comes down to leadership and having that focal point within the Department that other agencies can look at across the Federal Government, as well as individuals in the private sector. And that is absent now. That is why we have this drift.

Now, is the Department of Homeland Security ultimately responsible for removing all spyware or stopping all phishing and stopping all data warehouse issues? I would argue, frankly, no, at the end of the day. They have a leadership role, but that is largely the responsibility of the private sector. But, nonetheless, we need that focal point and leader within a department that people can turn to to pull together that overall strategy.

I would contend that the key priorities for the Department remain identifying that critical infrastructure that is so important to our economic and national security and working on communications, contingency plans, recovery plans. That is consistent with the mission of the Department; and that, to me, is what is absent today at the Department of Homeland Security.

Ms. ALLEN. I would just say I think there is a role for the DHS to play. Certainly on the identity theft issue, just as you said, it is a very complex issue. That is a crime that comes out of software vulnerabilities. It is a crime that comes out of processes that may be lax. It is something that is just not a financial services issue. And certainly our regulators are very active and very strongly sup-

porting those kinds of processes and technology changes that will help address some of the issues.

The problem is the data is out there. You can go on the Internet in a very short period of time and find out everything that you need to know about you. So the Internet has exacerbated the problem by making it easier to pull this information together. So it is a combination of educating, preparing people and consumers and businesses to understand what these threats are and how to prevent them from either a process or a technology point of view. It is a point of going after the software vulnerabilities and encouraging the providers of IT to close those gaps. It is an issue of best practices and policies that can be instituted in all kinds of institutions. And, most important, it is support of law enforcement, the people that are talking to you, letting them have both the knowledge and the resources to go after these fraudsters.

Ms. SANCHEZ. Thank you.

Thank you, Mr. Chairman, for the time. I appreciate it.

Mr. LUNGREN. Thank you.

And now the Chair recognizes the Chairman of the full committee, Mr. Cox.

Mr. COX. I thank the Chairman.

I want to thank, once again, each of our witnesses for your outstanding presentations.

I want to ask about the National Computer Security Division and ask you whether or not you agree or disagree with the position of the previous assistant secretary of homeland security for information analysis and infrastructure protection, who told us that keeping the National Computer Security Division under the assistant secretary for infrastructure protection was the correct thing to do. In the assistant secretary's view, its placement there allowed better integration of efforts to protect critical infrastructure from both physical and cyberthreats.

Do you agree or disagree with this position and why? And can you also add to that whether you see any ways to address perceived problems with integration? And, finally, could that integration occur at a higher level?

Yes, Mr. Kurtz.

Mr. KURTZ. I would respectfully disagree with the previous assistant secretary. I think the elegance of the bill that has been put together is that you don't lose the integration in what has been proposed. Under the bill, you have created a new assistant secretary that focuses on cybersecurity who works alongside an assistant secretary who presumably is working on physical security, and you have your information analysis assistant secretary working there as well. So you have three assistant secretaries working under an under secretary, and the under secretary can work to integrate programs and policies as appropriate.

So I think, you know, in my written remarks, in my oral remarks, I also think there is a fundamental misunderstanding of how we defend information networks versus physical assets which we require a different set of skill set. It is far more complex, I would argue, than securing a physical infrastructure. So I would—.

Mr. COX. And are you of the view that NCS would come under the new assistant secretary?

Mr. KURTZ. Most definitely, especially with the integration voice and data networks. I think it would be a mistake to leave the NCS out to the side.

I would note that when we talk about priority communications, which are the responsibility of the NCS, if you were to set that to the side in a VOIP environment, it would be very difficult and cumbersome to coordinate downstream. You need to—we need to recognize the confluence of telecom and IP networks and have the leadership in place to take care of it.

Ms. ALLEN. I would respectfully disagree, also. The reason is it is a different skill set in cybersecurity; and it is much more complex, as Paul mentioned, to understand the cybersecurity issues. And in a way the model of how the public-private sector works together is one of cooperation and collaboration. I don't see why that can't occur within the Department of Homeland Security; and I think it would be important for Congress to reward success in collaboration and problem solving and working together, as opposed to having silo approaches.

Lastly, let me address—the NCS I think is a fabulous organization. BITS has worked very closely with them on the telecom redundancy and diversity issues. They have been a key player in addressing some of the problems that we had after 9/11 with the business continuity issues, with the telecom industry, and I think they belong under the cybersecurity arena.

Mr. COX. Mr. Miller.

Mr. MILLER. Mr. Cox, the other point I would add, I totally agree with my colleagues, with all due respect to the former assistant secretary's view. But in addition why this is so important is the reason that Ms. Allen brought up so eloquently in her testimony is the cross-sectorial work. Not having an assistant secretary to bring the other government agencies together and get them to focus more on cyber in addition to physical is a problem.

Until yesterday, when my tenure ended, I spent the last 16 months chairing the Partnership For Critical Infrastructure Security, which is an organization of private sector representatives of each of the critical sectors. Until I brought Mr. Yoran to speak before them about a year and a half ago at one of our meetings, many of those other sectors had never even thought about the cyber issue, Ms. Allen's organization's being a great exception, because financial services does and telecommunications does, but many of the other sectors hadn't even thought about these issues. And the government agencies with which they liaise, Mr. Chairman, a lot of them don't have expertise internally. Having an assistant secretary at the Department of Homeland Security can help the other agencies do a better job in terms of working with these other critical sectors.

Mr. COX. I just want to note, Mr. Chairman, that the legislation that is before us would in fact give the assistant secretary primary authority within the Department over the National Communications System.

My time has expired.

Mr. LUNGREN. I thank you.

The Chair now recognizes the ranking member of the full committee, Mr. Thompson.

Mr. THOMPSON. Thank you, Mr. Chairman; I have an opening statement that I want to include in the record, rather, now at this time.

[The statement of Mr. Thompson follows:]

PREPARED STATEMENT OF THE HONORABLE BENNIE THOMPSON, RANKING MEMBER, COMMITTEE ON HOMELAND SECURITY

Thank you Mr. Chairman, Ranking Member Sanchez. I am glad we are here today to consider this important legislation.

H.R. 285 is an important step in fixing a very big problem at the Department of Homeland Security. It is clear from the Department's actions over the past two years that it does not consider cybersecurity to be an important issue.

For example, the last Director of the National Cybersecurity Division, Mr. Amit Yoran who is with us today, left last Fall ? and the Department has still made no attempt to identify a replacement.

In addition, the Department has moved slowly, if at all, to implement the goals set out in the *National Strategy to Secure Cyberspace.*

This inaction is inexcusable. Cybersecurity is about more than just the world of computers and hackers. In the 21st century, the prosperity of each and every American is dependent in one way or another on information technology, and those systems must be protected against breaches like the ones experienced by LexisNexis or ChoicePoint.

Vital assets such as the electric power grid, gas pipelines, nuclear power plants, and our air traffic control systems rely on the cyber infrastructure for operation. This is also true of vital government and military systems. With the ever-changing threats facing our cyber infrastructure, time is of the essence.

It is hard for me to understand how the Administration can be so reluctant on this issue, given the overwhelming support by the private sector, our colleagues across the aisle, and the Democrats in Congress.

Today, as we hear from the private sector, I hope to hear suggestions as to how the Department of Homeland Security can improve its strategy, management skills, and resource allocation to get the job done.

We also need to know whether, from your perspective, you think that the government is living up to its obligation in this public-private partnership. Is there someone in the government devoting 24-hours a day, 7 days a week to cybersecurity? If a cyberattack were to happen today, would we be ready for it?

When it comes to ensuring cybersecurity, I believe that government and industry must work together closely, and that this effort requires attention at the highest level in both the public and private sectors.

We can develop a culture of security within our computer networks and ensure our national security. But first, we must have effective leadership on cybersecurity issues at the Department and we must have that leadership now.

That is why I urge my colleagues, during the markup of H.R. 285 later today, to vote for this critical legislation. Thank you.

Mr. THOMPSON. Let me first compliment and congratulate Mr. Silva for his promotion. We all could benefit from such lofty movement. Congratulations.

And I want to compliment Ms. Lofgren and Mr. Thornberry for this bill. It is a wonderful bill. We have tried for a while to make it happen. There is no question about the fact that we need to elevate the position. In Washington, unless you are at a certain level, people don't pay you much attention. I think clearly the issue of cybersecurity has not been given the level of attention that it should have, and hopefully we will correct it.

With respect to merging cyber and physical infrastructure, is that something that individually you all see as something that is very positive for what is going on, or how do you see those two issues?

Mr. SILVA. I think we can't overlook the need to have at least close collaboration between the physical and the cyber side. I think, as my colleagues have already pointed out, there are clearly dif-

ferent disciplines there, but to spin cyber separate from physical I think would probably—I think what we don't want to do is we don't want to create too much of a disconnect between those two, because there is a relationship between the physical and the cyber, and I think it shouldn't be ignored. As we said in our testimony, or as I said in my testimony, it is very important that the leaders of both of those organizations, physical and cyber, be empowered individuals and be able to work closely together and coordinate their efforts in such a way that we don't sacrifice one for the other.

Mr. THOMPSON. Ms. Allen.

Ms. ALLEN. I think that there is an interdependency. Certainly, the systems that run much of our critical infrastructure are run off the same operating system that the financial services runs, that the first responders run. So we have to understand the interdependency that our industries, the physical industries have on the IT industry, the software operating systems, on the telecommunications and the power industries. Because if they are down or if there is a cascading effect of them being down, our physical structures as well as our cyberstructures are going to be—we will not be able to communicate. So I do think there need to be separate assistant secretary level positions, but I do think there needs to be the collaboration and cooperation in addressing the issues.

Mr. KURTZ. I would essentially agree with what Cathy has just pointed out. I think there is—if you pictured a physical infrastructure in one circle and the cyberinfrastructure in another, there is certainly some overlap between the two. But the disciplines through which you use to protract those infrastructures, to defend those infrastructures are very different. So, on the whole, yeah, there needs to be that integration under an under secretary type individual, but there is different disciplines involved in protection and defense.

Mr. YORAN. Sir, I would point out that, just as battle plans may include elements of air power, armor, sea power, intelligence, similarly we need integrated risk management practices. But all of those disciplines are highly specialized in and of themselves and need to remain specialized in order to be effective.

I would also—if I could just take a second or two to answer the previous question with a slightly different perspective, and that is it may have been possible that at the initial phases of the National Cyber Security Division it was a more effective strategy to make it part of infrastructure protection. Simply put, there was no organization. It was a from-ground-zero startup. We had to go in and recruit the individuals, and having a larger organization to participate in may have facilitated some growth and enabled us to build and accomplish what we were able to accomplish.

As Secretary Chertoff moves into his second stage review, I would say we also need to look at how in the current environment, not with legacy perspectives, we can integrate our cybercapabilities into a holistic risk management practice. This means having cybersecurity at the table along with physical security and participating in the grant programs, the emergency planning and readiness programs, the Office of Domestic Preparedness, and State and local programs across the Department and, just as importantly, alongside other departments and agencies. Many of the issues and

challenges mentioned earlier by my counterparts include many policy coordination roles in which the FDC, the Department of State, the Department of Justice, and Commerce have a primary regulatory or significant stake.

Mr. LUNGREN. Thank you very much.

The gentleman Mr. Pearce is recognized.

Mr. PEARCE. Thank you, Mr. Chairman.

Ms. Allen, you had stated that investor confidence and reliability of information systems are linked to the security and reliability. What countries are excelling in that particular relationship today, in security and reliability?

Ms. ALLEN. Well, the U.S. has the leadership. Even though we have headlines about breaches or problems that we have with cybersecurity, the U.S. has the most sophisticated people in terms of information security and IT. So if you look at best practices or you look at the development of software, anti-intrusion software or other types of software that help to prevent or identify breaches, it is mostly U.S. based.

Mr. PEARCE. Also, it would be useful to know, if I were to look at the nearest competition, how many laps behind us are they? Are they catching up, or is the rest of the world moving? Because as we look at the flows of financial capital, this is going to be the determining factor.

Ms. ALLEN. That is right. In the U.S., we fortunately have a good reputation in terms of the—and because of all the regulation that we have of the financial community and the economic system; and I think we will continue to enjoy that. The U.S. is light years ahead of regulators in other countries around regulating us against or for information security, information technology, all of the issues that help us to provide safety and soundness. So we are far ahead of any other country in that area.

There are other countries, however, that have the leadership role, so to speak, in the bad guys, the hackers and the countries where the ISPs, the Internet service providers, are not regulated or there is not oversight.

So I think we have a challenge in the U.S. to not only maintain leadership to maintain our economic livelihood, but we also have a challenge to help bring the other regulators and the other countries up to speed on these issues, and to help—to cooperate with them to go after the fraudsters and the hackers and the criminals.

Mr. PEARCE. Sure. Actually, the flows of financial capital have actually disciplined them very well. I am not so concerned that we bring them up, because simply the evaporation of capital from them as they fail to do their own internal strengthening is going to accomplish that. And we saw that even in the recent trip to South America and to some of the countries that have turned sharply to the left. Their political climate shifted to the left, but their business advisers, their economic advisers stayed solidly in the business sector. And that is with realization that we can talk what we want to in politics, but we had better keep our financial house moving forward.

You talked somewhat in your written testimony about market incentives, and I have got one more question for Mr. Silva. So if you

could give me a very brief description of the market incentives that you see available for these functions.

Ms. ALLEN. I think both R&D dollars that could help to encourage the development of technologies. Because, in the end, we are going to have to address this partially as a technological issue, the ability to have software that will counteract what is happening.

I think a second is tax incentives to build the critical infrastructures. Again, I come back to the telecommunications industry as one where we are all reliant on their diversity and resiliency, and we need—they are in dire need of help to develop that capability.

Mr. PEARCE. Thank you.

Mr. Silva, you talk about the essential information sharing and the fact that it has been hindered by the complex bureaucratic structure that mostly is worried about protecting people from lawsuits. How can we basically see that the new structure is free from those constraints?

Mr. SILVA. I think that particularly—some of this had been addressed a couple of years ago with some of the protections for FOIA protection and some other areas. But the problem is that when organizations want to share information with the government, the government either has to make it available to all of them or, if it chooses to provide that information only to a select few, then there are going to be issues that arise from that.

I mean, there are so many different organizations; and what tends to happen is when the information—whenever we create a new sharing relationship with an organization that seems to be at the exclusion of the other organizations—and this is very confusing to the various organizations. In fact, if you want to have your bases covered, you have to sort of join every organization to make sure that you are covered, and it is quite confusing. If the Department can establish a unified policy of sharing across the board with all of the organizations that are relevant, then I think that would go a long ways to solving that problem.

Mr. PEARCE. Thank you. Thank you, Mr. Chairman.

Mr. LUNGREN. The gentlelady from California, Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chairman. And I will be brief because I think the witnesses have covered the issues very well and thoroughly.

I would just note, as I said in my opening statement, that the staff on the subcommittee in the last Congress worked very hard and together. I mentioned Mr. Thornberry's excellent staff; and I see that Jessica Herrera who was his Democratic staffer, has also came. She also did a fabulous job, and I would like to publicly add my thanks to her along with Mr. Thornberry's staff.

As some of the witnesses have mentioned, there is much to do, I mean, from identifying and prioritizing the critical infrastructure in the cyberspace, to increased funding, to implementing the strategy. I mean, we are behind where we should be as a nation. And this bill alone doesn't solve that problem. What it does is set the stage to solve that problem, I believe.

We in the Congress cannot do the hire for this position. That would be inappropriate. But I think that we will give the Department an essential tool to recruit an excellent person, because the assistant secretary will have the clout and the prestige and the au-

thority to actually get the job done. I think that has been a frustration for those in the Department who have worked hard and who are smart people and who are skillful, but they haven't really had the ability to use their talents to move the country forward in a way that is so important.

Mr. Thornberry and I, at the end of the last Congress in December, issued a report of the activities and findings of the cybersecurity subcommittee, and I think some of the issues raised here today are really covered in that report in the to do list. I am hopeful that this subcommittee, although we have a very wide range of responsibilities, that we will have the time to schedule some hearings and some oversight on the elements that Mr. Thornberry and I identified in the last Congress.

The General Accounting Office is coming back with reports to us on some of the issues. One I think has just been received in draft form, and we will be receiving another. They are very helpful. We know that we need to pay some attention to whether or not we need to act to provide incentives for market solutions. I mean, there are differences of opinion that are valid, but we need—we have not seen the market move forward in the way that we had expected. I think we need to explore why that has happened and whether there is anything we can or should do about that.

The one thing we do know is that we don't want a heavy legislative regulatory approach to this, because our lawmaking will never catch up with the code writers. I mean, we really need to use market incentives in the leadership of the Federal Government in ways that are successful.

There isn't enough time to really go through how much needs to be done. In addition to the reach efforts that have been mentioned here, I am very grateful to NSF for stepping up to the bat, but clearly there are things that the Department needs to do. So I am pleased to be here today. I look forward to the markup later today, and I would yield back the balance of my time with thanks, Mr. Chairman.

Mr. LUNGREN. Thank you very much.

Mr. Jindal.

Mr. JINDAL. I have two quick questions. The first was regarding—Ms. Allen talked about the international marketplace, international response to the issue of cyberterrorism. I am wondering, is there a need for more coordinated international response given the fact that maybe attacks may be launched abroad because of the lack of protection overseas? Is there more that could be done? Or what can be done?

And the second question—I will go ahead and ask both my questions, also building on this question, about the legal liability. My question was, how is the insurance industry responding to this? Have they created products for the private sector to insure against these kinds of risks? If they haven't, what can we do to help integration of those products?

Ms. ALLEN. I am going to answer both quickly, and I am going to defer to Paul on one of the issues of what we can do on an international basis.

The answer is, yes, there is much more that we need to do on an international basis, not only cooperation with the laws but also

with law enforcement. Most of the phishing attacks that occur in the U.S. are launched from overseas. Most of the phishing attacks that come from the U.S. are launched on overseas institutions, and we have got to cooperate and try to shut down these fraudsters. So it is a higher level of cooperation; and I know Paul will tell you exactly, or at least one way to do that.

Secondly, on your question on market incentives. Yes, the insurance industry is developing products that will help to ensure best practices or appropriate behaviors of institutions, not just financial institutions, but all institutions, practices in cybersecurity. I think most of you know, on the legal liability side, the financial institutions are by law required to make all customers whole if there is any problem in an electronic delivery or an electronic transaction. Not all other countries have that same restriction. So it is also one of the things that makes us a target for potential fraud. There is much to do here, but we are looking at market incentives from the insurance industry to help move companies along.

Mr. JINDAL. Thank you.

Mr. SILVA. So, while I have the mike on my end, actually, some of the insurance companies have started market incentives already. In fact, AIG, which is one of our member companies, actually offers discounts to companies that adhere to a set of best practices. Now, while this is certainly not an end all to everything, I think it is an example of a market incentive which has a very positive effect and I think offers a reasonable reward to companies that are willing to take the steps. So I think that it is just starting. It is just starting.

Mr. MILLER. On the international, just coincidentally this week there is actually a meeting going on in Delhi between officials of the U.S. government, the Indian government, the U.S. IT industry, the U.S. financial services industry, and the industry of India, because India has become such a destination for so much offshore work.

But I would certainly agree, we are really in the infancy in the international cooperation. In addition to my chairing the U.S. IT association, I chair an international organization which is 65 countries. I spend a lot of time traveling around the world. And this issue simply hasn't raised itself at a higher level in other countries.

In the IT industry, and most customers, as Ms. Allen said in an earlier response to Mr. Pearce's question, certainly in the financial services industry, the U.S. is far ahead.

And, again, while the DHS has domestic responsibility, I would contend that having an assistant secretary—to come back to the purpose of the hearing—would help to elevate the issue. The State Department is doing some good work in holding bilateral meetings with other countries around the world. The Department of Justice, the Cyber Crime Division, has been doing some work with the G8 and other countries. But I think having someone at DHS at a higher position would help the internationalization of the need to collaborate on these issues.

Mr. KURTZ. I will just expand on what has been said.

I worked a lot on international issues when I was at the White House and did some of the initial trips at India and other places to foster international cooperation. At the time, we had a good pedestal to stand on. We had a national cybersecurity czar. We had a

special adviser to the President. We don't have that now. It is hard for us to make the point to other countries that they need to organize and react when we ourselves are not in the position we used to be. This is where I go to Harris's point. Having an assistant secretary would help us in this space.

Second point, the Council of Europe Convention on Cyber Crime, negotiated under President Clinton, signed under President Bush, it is in with the Senate. We would urge ratification of the Council of Europe Convention on Cyber Crime. I believe Business Software Alliance, ITAA, BITS, and a few other organizations have come together to say, to urge for ratification of this convention. What will that do? It will put in place that global framework for us to go after excuse me, for law enforcement to go after and prosecute cybercriminals abroad. We don't have that framework now.

Finally, on the insurance question. There is insurance out there. I think the problem has been there is no actuarial data available, or very little, which means there needs to be some sort of best practice or standard put in place. And I think until we have that best practice or standard in place that can be more widely adopted, we aren't going to see the insurance industry be all it can be, if you will, in that space.

Mr. JINDAL. Thank you.

Mr. LUNGREN. The gentleman's time has expired.

We thank all the panelists, all the witnesses for their valuable testimony and the members for their questions. Members of the committee may have some additional questions for the witnesses, and they may submit them in writing to you. We would ask you to respond to them, if you can.

The hearing record will be held open for 10 days.

The subcommittee stands adjourned. We are going to be meeting at 2:00 for markup on this. Thank you very much.

[Whereupon, at 12:36 p.m., the subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE RECORD

QUESTIONS SUBMITTED BY THE HONORABLE JAMES R. LANGEVIN FOR CATHERINE A. ALLEN

Question 1: One thing I have heard consistently over the past two years is that government regulation is the wrong way to bolster cyber security. The argument is that the government cannot move nearly as rapidly as market forces where it comes to information systems and security. Best practices are frequently used to demonstrate how the private sector is working to encourage a culture of security, except that it seems they are not updated as often as may be needed. This begs the question of whether these should be standardized by a group like NIST or not. I would like the panel's honest assessment of what the government's role in cybersecurity.

Answer 1: Financial institutions are heavily regulated and actively supervised at the federal level by the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of Currency, Office of Thrift Supervision, National Credit Union Administration, and the Securities and Exchange Commission and at the state level by numerous state banking and insurance commissioners. In recent years, these regulators have stepped up their oversight on business continuity, information security, third party service providers, and critical infrastructure protection. The financial services industry is working consistently and diligently to comply with new regulations and ongoing examinations. In addition, BITS and other industry associations have developed and disseminated voluntary guidelines and best practices as part of a coordinated effort to strengthen all critical players in the financial sector.

The financial services industry has been aggressive in its efforts to strengthen cyber security. We are sharing information, analyzing threats, urging the software and technology companies to do more to provide more secure products and services, and to combat fraud and identity theft.

Regardless of how well financial institutions respond to regulations, we simply cannot address these problems alone. Our partners in other critical industry sectors—particularly the telecommunications and software industries which are not regulated from a safety and soundness or data protection perspective—must do their fair share to ensure the soundness of our nation's critical infrastructure.

Our nation's economic and national security relies on the security, reliability, recoverability, continuity, and maintenance of information systems. IT security has a direct and profound impact on the government and private sectors, and the nation's critical infrastructure. Further, the security and reliability of information systems is increasingly linked to consumer and investor confidence. In recent years, members of the user community that rely on technology provided by the IT industry—private-sector companies, universities and government agencies—are demanding greater *accountability* for the security of IT products and services.

The federal government can play an important role in protecting the nation's IT assets. The following are seven key elements that the U.S. government should support to secure information technology. I refer to these as PREPARE, which is an acronym based on the first letter of each element.

Promote. Government can play an important role in promoting the importance of secure information technology. Also, government should do more to facilitate collaboration among critical infrastructure sectors and government. Some sectors, such as financial services, are heavily regulated and supervised to ensure that customer information is protected and that financial institutions operate in a safe and sound manner. Examples of actions the government can take include:

- Government should lead by example by ensuring that the issue of cyber security receives adequate attention in the Department of Homeland Security.

Today, cyber security is handled at a level far below where most corporations handle these issues. Congress could create a more senior-level policy level position within DHS to address cyber security issues and concerns and ensure that adequate funding is provided.

• Strengthen information sharing coordination mechanisms, such as the Information Sharing and Analysis Centers (ISACs), by ensuring adequate funding is made available to Federal agencies sponsoring such organizations. Information sharing and trend analysis within a sector is essential to protecting information security and responding to events. Information sharing among sectors is equally important as cyber threats sometimes reach some sectors before others.

• Create an emergency communication and reconstitution system in the event of a major cyber attack or disruption of information networks. Such an attack or disruption could potentially cripple many of the primary communication channels. To allow maximum efficiency of information dissemination to key individuals in such an event, a thorough and systematic plan should be in place. The financial services industry has developed such a plan for industry-specific events in the BITS/FSR Crisis Communicator. Other organizations have developed similar communication mechanisms. These emergency communications programs should be examined as potential models for a national cyber security emergency communication system.

• Reform of the Common Criteria/National Information Assurance Partnership (NIAP). The current software certification process is costly, inefficient, used on a limited basis by the Federal government, and virtually unknown to the private sector. NIAP should be reformed so that it is more cost effective for vendors to seek certification while ensuring consistent Federal procurement practices and expanded commercial adoption of NIAP-certified products. The BITS Product Certification Program may well be able to serve as a model.

Responsibility. Government should promote shared responsibility between suppliers and end users for developing, deploying, and maintaining secure information networks. Government can play an important role in establishing incentives and making producers of software and hardware accountable for the quality of their products. Examples of actions the government can take include:

• Provide tax or other incentives for achieving higher levels of Common Criteria certification. Incremented incentives would help to compensate companies for the time and cost of certification. This should encourage certification and increase the overall security of hardware and software.

• Provide tax or other incentives for certification of revised or updated versions of previously certified software. Under Common Criteria, certification of updated versions is costly and time consuming. Incentives are necessary to ensure that all software is tested for security

• Require software providers to immediately notify ISACs of newly discovered cyber threats and to provide updated information on such threats until an effective patch is provided. It is vital that critical infrastructure companies receive immediate notice of serious vulnerabilities.

• Establish requirements that improve the patch-management process to make it more secure and efficient and less costly to organizations.

Educate. Communicate to all users of information technology the importance of safe practices. Public confidence in e-commerce and e-government is threatened by malicious code vulnerabilities, online fraud, phishing, spam, spyware, etc. Ensuring that users (home users, businesses of all sizes, and government) are aware of the risks and take appropriate precautions is an important role for government and the private sector. Examples of actions the government can take include:

• Fund joint FTC/DHS consumer cyber security awareness campaign. The FTC should focus its efforts on building consumer awareness, and DHS should coordinate more detailed technical education regarding specific serious threats. In addition, government employees should be trained in proper cyber safety measures.

• Train government employees on proper cyber security measures.

• Educate corporate executives and officers regarding their duties under Sarbanes-Oxley, GLBA, and HIPAA as they relate to cyber security.

Procure. Using its purchasing power and leveraging security requirements and best practices developed by the public and private sectors, government can play an important role in encouraging the IT industry to deliver and implement more secure systems. Examples of actions the government can take include:

• Require high levels of cyber security in software purchased by the government through procurement procedures. Extend such requirements to software used by government contractors, subcontractors, and suppliers.

- Provide NIST with adequate resources to develop minimum cyber security requirements for government procurement. NIST should include software developers and other stakeholders in the standard-creation process.

Analyze. Government should collect information and analyze the costs and impact of information security risks, vulnerabilities and threats and provide this analysis to policy makers. Examples of actions the government can take include:

- Assign to the Commerce Department or another appropriate agency the responsibility of tracking and reporting such costs and their impact on the economy. Measuring and making these costs transparent will aid law makers and regulators as they assign resources to cyber security programs.

Research. Government can play an important role in funding R&D in the development of more secure software development practices, testing and certification programs. In addition, training future generations of programmers, technicians and business leaders that understand and manage information security can be accomplished by establishing university and educational/certification programs. Government can help by facilitating collaboration with the users and suppliers of IT to develop standards for safe practices. Examples of actions the government can take include:

- Enhance DHS, NSF, and DARPA cyber security R&D funding.
- Carefully manage long- and short-term R&D to avoid duplication.
- Establish a mechanism to share educational training and curricula.

Enforce. Law enforcement must do more to enforce, investigate and prosecute cyber crimes here and abroad. Examples of actions the government can take include:

- Ratify the Council of Europe's Convention on Cybercrime.
- Enhance criminal penalties for cyber crimes.
- Make cyber crimes and identity theft enforcement a priority among law enforcement agencies.
- Encourage better coordination among law enforcement agencies in order to detect trends.

Question: 2: If you do not want regulation, what do you want? Can DHS actually have an impact if it is only a coordinator and not an enforcer? Do you feel it is possible to draft regulations that would require minimum security standards, or would that encourage complacency?

Answer 2: Financial institutions are heavily regulated so no additional regulation of financial institutions is warranted. Financial institutions view the question as how best to urge the software industry, telecommunications industry and power industry to take greater responsibility for their products and services. It is important for members of Congress and the Administration to recognize the dependence of all critical infrastructures on software operating systems and the Internet. Given this dependence, the Congress should encourage providers of software to the financial services industry to accept responsibility for the role their products and services play in supporting the nation's critical infrastructure. In so doing, Congress should support measures that make producers of software more accountable for the quality of their products and provide incentives such as tax incentives, cyber-insurance, liability/safe harbor/tort reform, and certification programs that encourage implementation of more secure software. Congress also could provide protection from U.S. antitrust laws for critical infrastructure industry groups that agree on baseline security specifications for the software and hardware that they purchase.

In addition, DHS can encourage collaboration and coordination among other critical infrastructure sectors and government agencies to enhance the diversity and resiliency of the telecommunications infrastructure. For example, the government should ensure that critical telecommunications circuits are adequately protected and that redundancy and diversity in the telecommunications networks are assured. Further, the Congress should encourage law enforcement to prosecute cyber criminals and identity thieves, and publicize U.S. government efforts to do so. These efforts help to reassure the public and businesses that the Internet is a safe place and electronic commerce is an important part of the nation's economy.

Since its creation in 2003, DHS has focused primarily on physical security. It has not focused enough attention on addressing cyber security concerns. Elevating the cyber security position is a small step as part of a broader strategy to strengthen cyber security. Cyber security issues are handled in the government at a level far below where most corporations in the private sector handle these issues today. Elevating this critical position and ensuring that adequate funding is provided will help to focus greater attention on cyber security issues within the government and throughout the private sector and thus implement many areas identified in the Administration's National Strategy to Secure Cyberspace.

Since its creation, DHS has devoted substantial resources in bringing interested parties together to discuss cyber security risks. For example, DHS has hosted or supported fora to discuss steps that government and the private sector can and should do to mitigate cyber security risks. However, DHS has not devoted enough resources to address other key components of securing cyberspace. This include efforts to raise awareness of cyber security risks and steps consumers can take to protect themselves, facilitating collaboration among critical infrastructure sectors and government, strengthening a information sharing coordination mechanisms, such as the Information Sharing and Analysis Centers (ISACs), reforming the Common Criteria/National Information Assurance Partnership (NIAP), and urging the IT industry to take on greater responsibility for the security/quality of its products and services.

Question 3: Ms. Allen, I would like to get your opinion on the recent joint rules made by the FDIC, Comptroller of the Currency and other agencies regarding data theft at financial institutions. Do you believe they overstepped their bounds by doing this? If so, how do you feel this growing problem should be dealt with?

Answer 3: The federal financial regulators issued a final rule on customer notice breach requirements in March 2005 following a notice and comment period. About 80 organizations submitted comment letters, including BITS and The Financial Services Roundtable. Fortunately, the regulators responded to some of the concerns voiced in these comment letters. Consequently, the regulators provided greater flexibility for financial institutions when deciding when and how best to notify customers in response to a security breach.

Notifying customers is a complicated and complex process and can, if poorly done, undermine confidence in the financial services industry. Care must be exercised in alerting consumers to steps they can take to protect themselves from ID theft and other forms of fraud while averting needless alarm.

Members of BITS and The Financial Services Roundtable believe financial institutions have a strong track record in protecting customer information and in communicating with customers when security concerns arise. Protecting customer information is of paramount concern and our member institutions have taken a proactive approach in this regard. Examples of these efforts include the creation of the Identity Theft Assistance Center (ITAC) as well as BITS guidelines and best practices for reducing fraud, managing third party providers, engaging law enforcement agencies, and communicating with customers.

We believe that financial institutions should have the flexibility to develop their own risk-based approaches toward dealing with unauthorized access to customer information, whether at their own operations or with a third party service provider, within the current guidelines set forth in section 501b of GLBA. For example, financial institutions should be given flexibility in determining a course of action when they "flag" and secure accounts that have been threatened.

Efforts by various states and regulatory agencies raise significant implementation problems for financial institutions. In a transient society, notification should occur uniformly regardless of which state the consumer may live in. Moreover, inconsistent application of inconsistent state law inevitably creates a compliance nightmare for institutions with a multi-state presence.

Members of BITS and The Roundtable believe it is important for legislators and regulators to adopt uniform national standards to avoid serious implementation problems and inconsistent applications. Our members also encourage legislators and regulators to mandate notification only when there is some indication that the breach actually has the potential to cause harm or injury. If harm is demonstrably contained, for example, and no risk really exists, there should not be any reason to notify and scare people. Moreover, we believe it is wise policy that legislators and regulators require companies that discover breaches in security to immediately notify law enforcement authorities, as well as consumer reporting agencies, so that law enforcement authority can get a jump on any existing criminality and Credit Reporting Agencies may be better prepared for the potential volume of consumer inquiries about the impact of any breach on consumer credit history. Further, BITS and the Roundtable support measures to impose caps on damages. Any allowable damages should have firm caps and there should be no damages absent a showing of intent or actual harm. Absent negligence, an affirmative defense should be available if the company can demonstrate that is it a victim of fraud. Other measures include providing "safe harbors" from lawsuits for companies if they have instituted reasonable internal notification procedures.

QUESTIONS SUBMITTED BY THE HONORABLE DANIEL LUNGREN FOR PAUL B. KURT

Question: 1. What is the Government's role in cybersecurity? If you don't want regulation, what do you want? Can DHS actually have an impact if it is only a coordinator and not an enforcer? Do you feel is it possible to draft regulations that would require minimum security standards, or would that encourage complacency?

Government's Role in Cybersecurity

The Federal Government is positioned to assist with forensics, attack attribution, protection of networks and systems critical to national security, indications and warnings, and protection against organized attacks capable of inflicting debilitating damage to the economy. Additionally, Federal activities should also support research and development that will enable the private sector to better secure privately-owned portions of the nation's critical infrastructure.

Three Federal documents provide a framework for Federal responsibilities to secure cyberspace:

- *The President's National Strategy to Secure Cyberspace* (February 14,2003)
- *Homeland Security Presidential Directive-7 (HSPD–7)* (December 17, 2003)
- *The National Response Plan's Cyber Incident Annex* (January 6, 2005)

The President's National Strategy to Secure Cyberspace provides clear policy guidance on the Federal government's role: "The policy of the United States is to protect against the *debilitating disruption* of the operation of information systems for critical infrastructures and, thereby, to help protect the people, economy, and national security of the United States. . . We must act to reduce our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our nation's *critical infrastructure* and ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable and cause the least damage possible."

HSPD–7 establishes the U.S. government's policy for the identification and protection of critical infrastructure from *terrorist* attacks. It focuses in large part on the identification and protection of assets that would cause catastrophic health effects or mass casualties if attacked, comparable to those from the use of a weapon of mass destruction.

Finally, *The National Response Plan's Cyber Incident Annex* upholds the President's National Strategy to Secure Cyberspace and HSPD–7. The NRP Cyber Incident Annex states that the Federal government plays a significant role in managing intergovernmental coordination (Federal, state, local and tribal) and, where appropriate, public-private coordination in response to cyber incidents of *national significance.*

Ultimately, Federal activity is bounded by these three documents to protecting against debilitating attacks against critical infrastructure, attack attribution for national security systems, forensics, and research and development.

The DHS Impact

The Department of Homeland Security (DHS), as designated by HSPD–7 and the National Strategy, is the government's focal point for prevention, response and recovery from cyber security incidents that have a debilitating impact on our national and economic security. The Strategy sets specific responsibilities for the DHS, including:

- Developing a comprehensive plan to secure critical infrastructure
- Coordinating with other Federal agencies to provide specific warning information and advice about appropriate protective measures and countermeasures to state, local and nongovernmental organizations including the private sector, academia and the public.

DHS's responsibilities in the area of cyber security, although narrowly defined, are extremely significant to our economic and national security. DHS serves as the point of coordination for all government and national efforts. Senior DHS leadership, at the Assistant Secretary level or higher, is needed to build an effective government-private sector relationship, to understand the technical and global complexities of cyber security, and to marshal the resources necessary to provide an effective partnership with private sector organizations and initiatives.

Regulation

Regulation is difficult, due to rapid technology changes, and regulation can also stymie innovation. A report from the Business Roundtable (BRT) states, "traditional regulations directing how companies should configure their information systems and networks could discourage more effective and successful efforts by driving cyber security practices to a lowest common denominator, which evolving technology would quickly marginalize." A regulatory approach could result in more homogeneous secu-

rity architectures that are less secure than those currently deployed. Given the complexity and dynamism of cyberspace, the marketplace will provide in most cases the necessary impetus for improving IT security. In those instances where existing market forces fail to provide such impetus, incentive programs that rectify market shortfalls and encourage proactive security solutions should be considered and adopted as appropriate.

Minimum Standards

CSIA believes we should encourage the adoption of existing standards, rather than creating new ones. Several sets of standards and best practices exist today. Some are required under current regulation, such as Gramm-Leach-Bliley or the FDA Part 21, while others are voluntary, such as International Standards Organization (ISO) 17799, or Control Objectives for Information Technology and Related Systems (COBIT).

Question 2: What can be done to improve cybersecurity within the Government? Why is the Government's coordination so bad? Should DHS be responsible for the Federal government's cybersecurity, or should OMB retain this duty?

The Government has to address cybersecurity in a holistic manner, rather than attempting to solve each problem piece by piece. By securing entire networks from the ground up, coordination within the Government will improve.

To even begin to accomplish this, OMB needs to look to the authority it was granted in the Federal Information Security Management Act of 2002 (FISMA). FISMA positions OMB to strengthen the federal information security program, evaluation, and reporting requirements for federal agencies. However, this has not been achieved to its highest level, nor are there adequate—resources and personnel available to accomplish this. The security of Federal systems could be improved by ensuring OMB has more resources to ensure oversight of FISMA implementation.

The government needs to use the power of procurement to encourage vendors to provide products that meet a higher government standard. Subsequently, the government can coordinate to implement standard practices, procedures, and policies across all the federal agencies.

The security of Federal systems could also be improved by ensuring FISMA is more thoroughly applied to contractors supporting the Federal government. The GAO's recent report, "Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk" discusses this issue in detail.

Finally, GAO identifies in "Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements" the use of the annual "report card" on governmental information security as an effective tool to identify and address security weaknesses.

Question 3: Is the private sector doing enough to educate consumers and users about the importance of cyber security? There have been several studies recently that show most computer users do not take security very seriously. What can we do about this?

Based on the number of security breaches and increasing cases of identity theft, it is fair to say that consumers are not as educated on the importance of cybersecurity as they should be, leaving a large percentage of computers unprotected. The private sector has increased its efforts in recent years to educate consumers about cybersecurity issues. Primarily, the private sector has established partnerships with the major networking and operating system providers, which have eased the burden on the consumer, while working to secure cyberspace.

Awareness campaigns, such as October's National Cyber Security Awareness Month, have also helped in the effort. CSIA and the National CyberSecurity Alliance(NCSA), along with a number of other awareness organizations, work with the FTC, FBI, the Small Business Administration, the Department of Homeland Security, the Department of Commerce, and other government agencies at the federal, state, and local level to promote cyber security awareness.

In instances where existing market forces fail to provide adequate impetus, incentive programs that rectify market shortfalls and encourage proactive security solutions should be considered and adopted as appropriate. A recent Congressional Research Service Report discusses incentives that may be adopted to help foster cyber security.

Finally, Federal government's leadership, particularly through an Assistant Secretary position at DHS, fostering collaboration, reducing legal barriers, and leading by example, will continue to assist the private sector in educating consumers.

QUESTIONS SUBMITTED BY THE HONORABLE JAMES R. LANGEVIN FOR KEN SILVA

Questions: One thing I have heard consistently over the past two years is that government regulation is the wrong way to bolster cyber security. The argument is that government cannot move nearly as rapidly as market forces when it comes to information systems and security. Best practices are frequently used to demonstrate how the private sector is working to encourage a culture of security, except it seems they are not updated as often as may be needed. This begs the questions of weather these should be standardized by a group like NIST or not. I would like the panel's honest assessment of what the government's role in cyber security is.

***If you don't want regulation what do you want? Can DHS actually have an impact if it is only the coordinator and not the enforcer? Do you feel it is possible to draft regulations that would require minimum-security standards or would that encourage complacency?**

Answer: You are correct that there seems to be a fairly broad consensus not just in the private sector, but in the National Strategy to Secure Cyber Space published by the Bush Administration, that federal regulation is not the appropriate approach to improving cyber security.

However, it is not just because the regulatory process is slow. There are many other reasons as well.

I'm not sure the federal government is on very firm ground in asserting that if they, through NIST of any other mechanism, wrote standards that there would be dramatic improvement. After all, for the fifth consecutive year the average score of the 24 federal agencies, which are charged with meeting such federal standards for cyber security, was a D+.As bad as things are generally in the private sector, recent research shows there is a substantial minority of firms, probably about 20% who are doing an excellent job at cyber security by following best practices. I'm not aware that the federal government's record is nearly that good.

And, while it is fine to say that federal standards intent would only be to create a floor many feel that floor would, in reality, become a ceiling. The last thing we want in the cyber security field is something like we have in the campaign finance field where everyone claims they meet the federal standards and no one really believes the regulations are accomplishing their intended goals.

In the last Congress one of your colleagues, Congressman Adam Putnam, circulated a draft bill that would have attempted to layout a regulatory system. It was resoundingly opposed by virtually all segments of the industry.

In response Congressman Putnam appointed the Corporate Information Security Working Group (CISWG) to address the question you ask today. At the conclusion of that effort last year Chairman Putnam wrote of the CISWG group that: ″The corresponding recommendations have provided valuable information and have already produced a variety of initiatives that have made a measurable difference.″

The Internet Security Alliance was very active in that group and is responsible for some of theses initiatives. The co-chairs of the Committee on Incentives, Liability and Safe Harbors was co-chaired by my first Vice Chairman on the ISAlliance Board, Ty Sagalow of AIG, and our ISAlliance Chief Operating Officer, Larry Clinton.

15 different trade associations participated in the Incentives/Liability Sub Group and produced two fairly detailed reports go a long way toward answering your question. I am supplying the reports for the record.

Briefly the group first answered your question of why regulatory measures were inappropriate to address this issue. They provided a series of reasons including the following:

1. The traditional regulatory structure (i.e. FCC/SEC style regulation) is likely to be both ineffective and potentially counterproductive to the interests of implementing a comprehensive cyber security program.
2. A cyber security program based on positive incentives is more likely to generate safer and more attractive products. This will increase consumer and business confidence in advanced technology and result in a better environment for the American economy in general and American businesses and consumers in particular.
3. Traditional regulatory structures are likely to be ineffective because:
   - The international nature of the cyber security issue demands a cross-boarder solution which national legislation cannot achieve.
   - The ever-evolving nature of the Internet and the cyber security threat demands a solution that can be quickly adapted to changing circumstances which is inconsistent with the nature of the traditional regulatory structure.

- The current US political consensus is that regulation of the Internet is unwise and hence the time it may take to enact a regulatory structure may not be appropriate given the urgency of the worldwide cyber security problem.

4. Traditional regulatory approach to cyber security is potentially counterproductive because:

- The traditional regulatory structure is an open process of public comment and reply comments. Such a process could lead to providing a roadmap of vulnerabilities to nefarious parties intent on causing damage.
- Private industry is better able to innovate and maintain the array of tools necessary to adequately police Internet security. Relying on inadequate resources could lead to the unsophisticated decisions yielding less, rather than more security
- The political process by which traditional regulatory standards are reached encourages compromise rather than maximum effectiveness. Hence the political process could result in an inefficient program that could yield a false sense of security.
- Government regulation of technology may blunt innovation resulting in less consumer choice, economy and security.

5. Hence a program of positive incentives such as insurance incentives, liability incentives and tax incentives is likely to be an effective, comprehensive and ongoing program of managing the security risks consistent with the ever evolving and international nature of the technology and the threats to it.

Based on this assessment the CISWG concluded, as did the National Strategy to Secure Cyber Space, that the best approach would be for governments and industry to work together. Specifically, the Working Group outlined six different incentive programs that should be considered three of which would be led by industry and three of which would be led by government.

In summary they are:

Industry Led:

1. Development of Common Measurement Tools/Seal of Approval and Vendor Certification Programs
2. Better Use of Cyber insurance tied to best practice adoption
3. Development of market entry incentives

Government Led

1. Safe harbor/tort reform tied to best practice implementation
2. Tax incentives
3. Credit programs such as FEMA credits or use of government procurement to drive better security in products sold

In the final phase of the CIWG process the group began to develop a new paradigm which could be used to drive best practice adoption on an international level by tying the various incentives into broadly adopted best practices which would use market forces to continually generate updates and modernizations.

The Sub-Group found that within the marketplace there already exists a robust assortment of published regulations, standards, best practices, and similar guidance. Research shows that compliance with these existing practices can result in demonstrable improvements in cyber security. Indeed, the largest study in the field to date found that the approximately 20% of companies deemed the ″best practices group″ suffered less monetary damage and downtime than less careful corporations, and one-third of this group suffered no such inconvenience despite being targeted by attackers regularly.

Further, the Group found that while there are apparently effective best information security practices operative in the world, there is still a consensus that no one size fits all. What qualifies for a specific entity, as a best practice will be affected by size of the entity, the culture or cultures it operates within, its sector specific regulatory status, and a range of other variables?

Government's role in the public-private partnership is to fashion an incentive program for the good actors that will create a business advantage for them over less careful players. In so doing, we hope to harness the power of the market to motivate cyber security.

The group specifically did not endorse the creation of a federally specified standard of information security to be applied to the vast private sector. Rather they were concerned that such an approach would be too static and could put U.S. business at a competitive disadvantage. Such an approach also might not be appropriate across various sectors, might be weaker than needed due to the political nature of the regulatory process, and hence, could be counter productive. It would also be very hard to enact legislatively.

Instead, they proposed that companies have available federal incentives if they implement information security pursuant to and meet the:

- Information security procedures adopted by a Federal sector-specific regulatory agency.
- Standards established and maintained by the following recognized standards organizations:
  - International Organization for Standardization
  - American National Standards Institute
  - Electronic Industries Alliance
- National Institute of Standards and Technology
- Standards established and maintained by an accredited security certification organization or a self-regulatory organization such as NASD, BITS, or the emerging CISP structure.

Finally, the Sub-Group analyzed the various types of incentives available and proposes a series of classes for organizing these incentives with the greater ability of an entity to demonstrate performance of agreed upon security practices yielding greater benefit. These incentives and their classification will require further analysis as part of the enactment process security controls pursuant to the identified standards should not be considered as conducting an unfair or deceptive practice. Similar state-based claims would also be preempted.

These benefits include:

- Limits on FTC Jurisdiction—a company that demonstrates it implemented information security controls pursuant to the identified standards should not be considered as conducting an unfair or deceptive practice. Similar state-based claims would also be preempted.
- Limits on State Actions—Once a company has demonstrated it has met the security requirements, then plaintiffs should face additional burdens, such as increases in the burdens of proof, caps on punitive damages, prohibitions on third-party liability, prelitigation notice requirements, or a cap on damages.

In summary Mr. Langevin, the Internet is a new type of technology that will require different methods of management and assurance than those that have been applied to previous technologies. Federal standards, for the reasons cited, above are not the answer.

This is not to say that the government, and governnient agencies such as NIST have no role. Quite the contrary, they have a very important role working with the private sector as part of a new model to insure long term information security.

The Internet Security Alliance would be pleased to work with the Committee in further developing this new model.