THE INVISIBLE BATTLEGROUND

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH AND DEVELOPMENT

OF THE

SELECT COMMITTEE ON HOMELAND SECURITY

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

SEPTEMBER 16, 2003

Serial No. 108–26

Printed for the use of the Select Committee on Homeland Security

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

---

U.S. GOVERNMENT PRINTING OFFICE

21–354 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

SELECT COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, Chairman

JENNIFER DUNN, Washington
C.W. BILL YOUNG, Florida
DON YOUNG, Alaska
F. JAMES SENSENBRENNER, JR., Wisconsin
W.J. (BILLY) TAUZIN, Louisiana
DAVID DREIER, California
DUNCAN HUNTER, California
HAROLD ROGERS, Kentucky
SHERWOOD BOEHLERT, New York
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
PORTER J. GOSS, Florida
DAVE CAMP, Michigan
LINCOLN DIAZ-BALART, Florida
BOB GOODLATTE, Virginia
ERNEST J. ISTOOK, Jr., Oklahoma
PETER T. KING, New York
JOHN LINDER, Georgia
JOHN B. SHADEGG, Arizona
MARK E. SOUDER, Indiana
MAC THORNBERRY, Texas
JIM GIBBONS, Nevada
KAY GRANGER, Texas
PETE SESSIONS, Texas
JOHN E. SWEENEY, New York

JIM TURNER, Texas, Ranking Member
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
BARNEY FRANK, Massachusetts
JANE HARMAN, California
BENJAMIN L. CARDIN, Maryland
LOUISE MCINTOSH SLAUGHTER, New York
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ROBERT E. ANDREWS, New Jersey
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
KAREN MCCARTHY, Missouri
SHEILA JACKSON-LEE, Texas
BILL PASCRELL, JR., New Jersey
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
CHARLES GONZALEZ, Texas
KEN LUCAS, Kentucky
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida

JOHN GANNON, *Chief of Staff*
UTTAM DHILLON, *Chief Counsel and Deputy Staff Director*
DAVID H. SCHANZER, *Democrat Staff Director*
MICHAEL S. TWINCHEK, *Chief Clerk*

Subcommittee on Cybersecurity, Science, and Research and Development

MAC THORNBERRY, Texas, *Chairman*

PETE SESSIONS, Texas, *Vice Chairman*
SHERWOOD BOEHLERT, New York
LAMAR SMITH, Texas
CURT WELDON, Pennsylvania
DAVE CAMP, Michigan
ROBERT W. GOODLATTE, Virginia
PETER KING, New York
JOHN LINDER, Georgia
MARK SOUDER, Indiana
JIM GIBBONS, Nevada
KAY GRANGER, Texas
CHRISTOPHER COX, California, *ex officio*

ZOE LOFGREN, California
LORETTA SANCHEZ, California
ROBERT E. ANDREWS, New Jersey
SHEILA JACKSON-LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
KEN LUCAS, KENTUCKY
JAMES R. LANGEVIN, Rhode Island
KENDRICK B. MEEK, Florida
CHARLES GONZALEZ, Texas
JIM TURNER, TEXAS, *ex officio*

CONTENTS

Page

STATEMENTS

The Honorable Mac Thornberry, a Representative in Congress From the State of Texas, and Chairman, Cybersecurity, Science, and Research and Development 1
The Honorable Zoe Lofgren, a Representative in Congress From the State of California, and Ranking Member, Cybersecurity, Science, and Research and Development
Oral Statement 2
Prepared Statement 5
The Honorable Donna M. Christensen, a Delegate From the U.S. Virgin Islands 24
The Honorable Jennifer Dunn, a Representative in Congress From the State of Washington 4
The Honorable Bob Etheridge, a Representative in Congress From the State of North Carolina 20
The Honorable James R. Langevin, a Representative in Congress From the State of Rhode Island
Oral Statement 33
Prepared Statement 6
The Honorable Sheila Jackson-Lee, a Representative in Congress From the State of Texas
Oral Statement 29
Prepared Statement 6
The Honorable John Linder, a Representative in Congress From the State of Georgia 23
The Honorable Ken Lucas, a Representative in Congress From the State of Kentucky 26
The Honorable Kendrick B. Meek, a Representative in Congress From the State of Florida 37
The Honorable Pete Sessions, a Representative in Congress From the State of Texas 27

WITNESS

The Honorable Robert Liscouski, Assistant Secretary, Infrastructure Protection Directorate, Department of Homeland Security
Oral Statement 7
Prepared Statement 9

WHAT THE DEPARTMENT OF HOMELAND SECURITY IS DOING TO MAKE AMERICA'S CYBERSPACE MORE SECURE

Tuesday, September 16, 2003

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CYBERSECURITY,
SCIENCE, AND RESEARCH AND DEVELOPMENT,
SELECT COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The committee met, pursuant to call, at 9:30 a.m., in Room 2118, Rayburn House Office Building, Hon. Mac Thornberry [chairman of the subcommittee] presiding.

Present: Representatives Thornberry, Sessions, Linder, Lofgren, Jackson–Lee, Christensen, Etheridge, Lucas, Langevin, and Meek.

Also Present: Representative Dunn.

Mr. THORNBERRY. The hearing will come to order. I would like to welcome our witness and guests to today's hearing, entitled The Invisible Battleground: What the Department of Homeland Security is Doing to Make America's Cybersecurity More Secure.

Over the past several months this subcommittee has received a number of perspectives on cybersecurity. We have held classified and unclassified briefings and hearings. We have heard from witnesses from academia, think tanks, technology industry, government agency, users, and others. Our goal has been to deepen our understanding of the issues involved and to gain a truer perspective on how and where cybersecurity fits into homeland security.

Now, today, we will hear a progress report from the new Department of Homeland Security.

From the first bills introduced in Congress to create a Department of Homeland Security, cybersecurity was one of those critical elements that was given to the new department, one of the functions where a number of government agencies would be brought together with greater emphasis and broader responsibilities. It was clear that if we were really going to modernize and strengthen Homeland Security, cybersecurity had to be a part of it.

The final legislation, in fact, did that. It did not set cybersecurity apart, as some proposed, but included it as one of the critical infrastructures placed under the Directorate for Information Analysis and Infrastructure Protection.

Since the Department began operations in March this year, it has brought some key people on board, although sometimes it has seemed to have taken a while. In June, it announced the creation of a National Cybersecurity Division; just yesterday a director was

announced for that division. Yesterday, also, an emergency response partnership with Carnegie Mellon University and a US–CERT was announced. So significant steps have been taken.

In its strategy, released in February, the administration acknowledged that cyberspace is the nervous system of the other infrastructures, the control system of the country. Thus, the healthy functioning of cyberspace is essential to our economy and our national security.

In our hearings so far, we have heard that cyber attacks are growing in number and complexity and in severity of the consequences. The recent bout with viruses and worms have shown that once they are launched, they are not easily contained; and as recently as last week, our hearing on the recent blackouts have shown again the interconnectiveness of various infrastructures. And yet there has been a lingering concern that cybersecurity has not been given the priority it deserves from the Department.

Today, we are ready to hear from the administration on some answers to these important questions, such as: Where are we in implementing each of the five priorities contained in the national strategy;

What can and should the Federal Government do to require or encourage better security for all of the IT infrastructure which is in private hands; and

What about the human element where we have received testimony that up to two-thirds of the problems that are created are created by the interface of human beings with technology?

In today's world, our computers and cyber networks are not just a place to do business and conduct research and communicate with our friends. Cyberspace is an invisible battleground that we must secure and defend, for attacks are being launched against us every day attacks against the central nervous system of the country and against our economy and our security. We must be ready. And today we hope to hear from our witness that we are in better shape than we have been in the past.

Before we turn to our witness, I am going to yield to our distinguished ranking member, my partner in this effort, Ms. Lofgren.

Ms. LOFGREN. Thank you, Chairman Thornberry, for holding this hearing and for your continued outstanding leadership of this committee.

I think the chairman did a great job in summarizing the work that this subcommittee has done to date. All the members of the subcommittee have taken the time to study this incredibly complex set of issues involving cybersecurity, and we certainly know more now than we did when we began our endeavor.

I think all of us agree that the Nation's cyber infrastructure remains vulnerable and that the Federal Government must provide leadership to better secure our systems in both the public and private sectors. My concerns about the Department of Homeland Security are that it is not providing sufficient leadership in the cyber arena, particularly in the following five areas:

Reducing vulnerabilities: The Department is tasked with reducing vulnerabilities to government in critical asset computers as well as responding to cyber incidents. The number of cyber attacks and resulting damage, however, continues to increase. This past

August was the worst ever for computer viruses. The Blaster, Welchia, and SoBigF viruses, along with other attacks, caused more than $32.8 billion in economic damages according to one digital risk assessments company.

Two, coordination: Is the National Cybersecurity Division coordinating with the private sector, other government agencies, and State and local governments to identify vulnerabilities? Has the NCSD begun a national risk assessment? If so, when will it be complete? I am concerned that the Department is not providing quick leadership in this area.

Departures from the administration: In the last 6 months the most senior Bush administration cyber officials have left the government. These individuals include Richard Clarke, the Special Advisor to the President for Cybersecurity; Howard Schmidt, the Vice Chair of the President's Critical Infrastructure Board, and Clarke's replacement; Ron Dick, the Director of the National Infrastructure Protection Center; and John Tritak, Director of the Critical Infrastructure Assurance Office. I am concerned about these departures and that the National Cybersecurity Division may lack sufficient personnel and resources to operate effectively.

Cyber priorities at DHS: Clearly, as the chairman has mentioned, cybersecurity is enormously important to the infrastructure of the Nation. I am worried that cybersecurity has been demoted in importance in the administration with the lead official for cyber issues reduced from a Special Advisor to the President, working in the White House, to a directorship very deep within the Department of Homeland Security. The Nation's cyber chief must have both the access and resources to do the job, the cyber chief at DHS.

It took the Department over 3 months to announce its choice for a leader of the NCSD. This delay is troublesome, and I am curious as to why it took the Department so long to settle on a candidate. I am also concerned about the number of other jobs that seem to be empty and vacant within NCSD, how many desks are empty. Is there anyone there to answer the phone?

With these concerns in mind, I am very encouraged by the person chosen to lead the NCSD. Mr. Yoran currently serves as the Vice President of Managed Security Services Operation at Semantech Corporation, the Internet security firm headquartered in Cupertino, California, near my home.

I am very familiar with the work of Semantech. It is one of the true bright spots in Silicon Valley, and its CEO, John Thompson, is a talented and thoughtful leader. I am hopeful that our new guy will provide needed leadership at the NCSD, and once he is on the job, I am going to tell him that he must candidly tell the chairman and me if he has the access and resources needed to accomplish his mission. If he is unable to do his job, Secretary Ridge should expect to hear from me and, I think, the chairman directly.

As you can see, we have many concerns about the cyber program of the Department of Homeland Security. I am pleased that we finally today will hear directly from the top official at DHS on our efforts. And the Assistant Secretary for Infrastructure has served as the acting chief since it was established on June 6, so I am sure he will address the concerns that I have raised; and I hope he will

be able to reassure me that cybersecurity is, in fact, a priority at the Department.

I thank the chairman for yielding.

Mr. THORNBERRY. Thank the gentlelady.

Without objection, the distinguished vice chair of the full committee will sit with the subcommittee today, and the Chair would yield to the gentlelady from Washington for any opening statement she would like to make.

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

Mr. Liscouski, I am looking forward to your testimony. Thank you for joining us here today. We are eager to learn about the Department of Homeland Security's most recent efforts, in fact, in June of this year to protect an important part of our Nation's critical infrastructure, our cyber systems.

In the wake of September 11, the leaders of this Nation have realized that securing our homeland against terrorist attacks also means that we need to think creatively about where our targets might be. We have visual reminders of many targets every single day. When we board an airplane, when we drive over a bridge, when we have our bags searched at football games.

But we also have targets that are far less visible. The power grid is one such example. Cyberspace is another. And that is why we are here today.

Your division, Mr. Liscouski, faces no small task. Securing cyberspace is an international issue, something I realized with greater awareness this summer when I addressed a group in London on cybersecurity, and was very happy to learn how involved the people of the British Government are in making sure we get this right.

Also, we know that a cyber attack from overseas cannot be intercepted at the border, or at least is very difficult to be intercepted at any border, since there are no borders in the cyber world.

This issue is also one that requires intense partnership with the private sector. The key to achieving a desired level of cybersecurity is utilizing and supporting the relationships that we have formed with the private sector, those on the ground doing research and development. Companies like Microsoft, which I represent here in the United States Congress, have realized that many of its priorities in business are in line with our Homeland Security priorities here in Congress. We are all working to prevent a situation where critical technological infrastructure is brought down.

This committee has spent a significant amount of time looking into the successful public-private and cross-industry partnerships that already exist. I hope the Department continues to work closely with the private sector to reach a clear understanding of what a safe network system looks like.

As the Department works to protect America's technological infrastructure, it also must keep in mind the interconnectivity these cyber connections have with the world's financial markets, transportation and communications systems.

I am very happy the Department is taking this charge seriously, and I look forward to your testimony.

Mr. THORNBERRY. Thank the gentlelady. Does any other member wish to offer an opening statement at this time?

Without objection, any member may submit an opening statement for the record.

[The information follows:]

PREPARED STATEMENT OF THE HONORABLE ZOE LOFGREN, RANKING MEMBER, SUBCOMMITTEE ON CYBERSECURITY, SCIENCE, AND RESEARCH AND DEVELOPMENT

Thank you Chairman Thornberry for holding this hearing and for your continued outstanding leadership of this subcommittee.

Chairman Thornberry did a terrific job in summarizing the work that this subcommittee has done to date. All Members of this subcommittee should be commended for taking the time to study the incredible complex set of issues involving cybersecurity.

We have learned a lot since this subcommittee first met at the beginning of the year. I think all would agree that our nation's cyber infrastructure remains vulnerable, and that the federal government must provide leadership to better secure our systems in both the public and private sector.

My concerns about the Department of Homeland Security are that it is just not providing sufficient leadership in the cyber arena, particularly in the following five areas.

- *Reducing Vulnerabilities:* The Department is tasked with reducing vulnerabilities to government and critical asset computers, as well as responding to cyber incidents. The number of cyber attacks, and resultant damage, however, continues to increase. This past August was the worst month ever for computer viruses. The Blaster, Welchia, and SoBig.F viruses, along with other attacks, caused more than $32.8 billion in economic damages, according to one digital risk assessment company.
- *Coordination:* Is the National Cyber Security Division (NCSD) coordinating with the private sector, other government agencies, and state and local governments to identify vulnerabilities? Has the NCSD begun a national risk assessment? If so, when will it be complete? I am very concerned that the Department is just not providing leadership in this area.
- *Bush Administration Departures:* In the last six months, the most senior Bush Administration cyber officials have left the government. These individuals include Richard Clarke, the special advisor to the president for cyber security; Howard Schmidt, the vice chair of the president's critical infrastructure board and Clarke's replacement; Ron Dick, the director of the National Infrastructure Protection Center; and John Tritak, director of the Critical Infrastructure Assurance Office.

I am very concerned about these departures and that the National Cyber Security Division may lack sufficient personnel and resources to operate effectively

- *Cyber priorities at DHS:* Clearly, cyber security has been demoted in importance in the Administration with the lead official for cyber issues reduced from a special advisor to the President working in the White House, to a Directorship buried deep within the Department of Homeland Security. The nation's cyber chief must have the both the access and resources to do the job.
- *Cyber Chief at DHS:* In addition, it took the department over 3 months to announce its choice for a leader of the NCSD. This delay is troublesome, and I am curious as to why it took the department so long to settle on a candidate. I am also concerned about the number of other jobs that need to be filled within the NCSD. How many desks are empty? Is there anyone there to answer the phone?
- With these concerns in mind, I am very encouraged by the person chosen to lead the NCSD. Mr. Amit Yoran currently serves as the Vice President of Managed Security Services Operations at Symantec Corporation, the internet security firm headquartered in Cupertino, California. I am very familiar with the work of Symantec. It remains one of the true bright spots in Silicon Valley, and its CEO, John Thompson is a talented and thoughtful leader.
- I am hopeful that Mr. Yoran will provide needed leadership in the NCSD. Once he in on the job, I am going to tell him that he must candidly tell me if he has the access and resources needed to do his job. If he is unable to do his job, Secretary Ridge should expect to hear directly from me.

As you can see, I have many concerns about the cyber program at the Department of Homeland Security. I am pleased that we finally get to hear directly from a top official at DHS today on its efforts. Robert Liscouski, Assistant Secretary for Infrastructure Protection, has served as the acting chief of the National Cyber Security Division (NCSD) since it was established on June 6, 2003.

I hope that Mr. Liscouski will address my many concerns and reassure me that cyber security is in fact a priority at the Department of Homeland Security.

PREPARED OPENING STATEMENT OF THE HONORABLE JAMES LANGEVIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF RHODE ISLAND

Thank you, Mr. Chairman. I would like to welcome Assistant Secretary Liscouski, and express my appreciation for your willingness to come here for what I expect will be a very informative and productive hearing. We have heard so much from both the private and academic sectors about the state of information security and their hopes and fears about the Department of Homeland Security's plans, and now we can find out about those plans directly from the source.

Mr. Chairman, my greatest concern by far is the fact that no information has been forthcoming from DHS until now. While I am pleased to finally get the chance to discuss how information security fits into the overall plan for critical infrastructure protection, I must express my disappointment at how long it has taken.

I believe it is the duty of this Subcommittee to determine what is being done, and what more can be done, to safeguard our critical infrastructure. While it is true that much of our information infrastructure lies with private industry, that should in no way reduce DHS's efforts to secure and protect it.

I am especially interested to hear Mr. Liscouski's opinion on whether or not the structure and resources being devoted to cybersecurity at DHS are sufficient to handle the tasks for which it is now responsible. In addition, I hope to learn what, if any, attention is being paid to home users and their security, an important group that is often left out of "big picture" views of information security. Most importantly, this Subcommittee needs to know how DHS can best work in conjunction with our computer industry partners and other agencies in order to raise the bar for information security for all users.

Again, I greatly appreciate Assistant Secretary Liscouski taking time to be here to discuss these vital issues with us.

Thank you, Mr. Chairman.

PREPARED OPENING STATEMENT OF THE HONORABLE SHEILA JACKSON-LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. Chairman, Thank you for calling this important and provocative hearing. With the recent blackouts, and the viruses which have been plaguing the House computer systems, our infrastructure networks—and our dependence on them—is abundantly clear. It will be good to explore what the Administration is doing to make them more secure.

Obviously, national security is foremost on everyon's minds these days. As we work to improve our country's security, it is important that we take inventory of all systems that are vital to the functioning of the nation, and do all we can to protect them. This certainly includes our computer networks systems that can be attacked anonymously and from far away. These networks are the glue that holds our nation's infrastructure together. An attack from cyberspace could jeopardize electric power grids, railways, hospitals and financial services, to name a few. The recent blackouts made it clear how fragile and vulnerable our infrastructure may be.

We are all aware of the growing number of internet security incidents. These incidents can come in many flavors: annoying attacks through emails, involving such things as computer viruses, denial of service attacks, and defaced web sites; or cyber-crime, such as identity theft. Such events have disrupted business and government activities, and have sometimes resulted in significant recovery costs.

Despite the risks, our hospitals and power grids, our communications, our transportation systems, will probably always be critically dependent on computers and information flow and the satellites above us. A terrorist or other criminal tampering with those systems could devastate entire industries and potentially cost lives. While we have been fortunate so far in avoiding a catastrophic cyber attack, Richard Clarke, the President's cyber-terrorism czar from last year, I guess I should say "two czars ago," said that the government must make cybersecurity a priority or face the possibility of a "Digital Pearl Harbor".

This was truly a frightening prospect. On paper, it seems we are taking bold steps toward securing cyberspace: we now have a National Cyber Security Division (NCSD) at the DHS, and its new U.S. Computer Emergency Response Team (US–CERT). I would like to thank Mr. Liscouski for taking the time away from the challenges that face him at the DHS to enlighten us on the progress the Department and the Administration are making on this important front.

We have been working on this subject for the past year in the Science Committee as well. One thing I have been disturbed by is the lack of good data on the threats that face us, and the absence of a solid assessment of the risks we face. How can we know how much to invest, and where, if we do not know those basics?

I want to know the magnitude of the threat out there, and how Americans are dealing with it. What is the role of the private sector, and of private citizens, and of the federal government? Are we putting adequate resources and energy into fulfilling that role?

I look forward to the dialogue. Thank you.

Mr. THORNBERRY. With that, we will turn to our witness. We want to welcome, Robert P. Liscouski, Assistant Secretary for Infrastructure Protection of the Department of Homeland Security.

I understand this is your first opportunity to testify in front of Congress. We appreciate your being here and you are recognized. Your full statement will be made part of the record, and you are recognized to summarize it as you wish.

STATEMENT OF THE HONORABLE ROBERT P. LISCOUSKI, ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. LISCOUSKI. Thank you and good morning, Chairman Thornberry and members of the committee. I am pleased to appear before you this morning to discuss some of our efforts to protect and secure our Nation's critical infrastructure.

From the beginning of DHS, IAIP and the Infrastructure Protection Office for which I am responsible recognized the equal importance of protecting physical as well as cyber assets. Thus, we created the National Cybersecurity Division on June 6 of this year. Today, I am here to give you a progress report on where we are now and where we will be going in the future to implement the President's national strategy to secure cyberspace.

Mr. THORNBERRY. Excuse me, Mr. Liscouski, would you pull the microphone just a little closer to you. It will be easier for us to hear. Thank you.

Mr. LISCOUSKI. All right.

I am pleased to announce this morning that Amit Yoran has been formally named as the Director of the NCSD, effective today. Mr. Yoran is a strategic thinker, a disciplined leader, who understands the unique threats and vulnerabilities manifested in cyberspace and is the individual who will further accelerate our efforts in building a full NCSD team and increasing the strength of our public and private sector partnerships.

Building upon the formation of the NCSD, the Department has worked to assemble a consolidated and coordinated team of cybersecurity professionals. Despite the many organizational and cultural challenges associated with integrating these elements into one entity, our initial efforts have yielded very effective positive and tangible results. The creation of the NCSD has enabled the initial consolidation of three 24x7 cyber watch capabilities; formulation of standardized incident handling procedures for responding to cybersecurity events; and the creation of a single national focal point for cybersecurity leadership for prevention, protection, and response to incidents.

The most recent accomplishments of the NCSD is the creation of the National Computer Emergency Response Team or the US–

CERT. The US–CERT, in collaboration with the private sector and leading response organizations, will improve warning and response time to security incidents by fostering the development of detection tools and utilizing common commercial incident and vulnerability reporting protocols. This will increase the flow of critical security information throughout the Internet community.

I would like to take a moment to address our rationale behind the decision to integrate physical and cybersecurity within the IAIP directorate. I believe that this approach is the correct one for three reasons.

First, cybersecurity cannot stand alone. The critical interdependencies between cyber and physical domains demand that we coordinate our intelligence and our protection efforts.

Second, with the creation of the NCSD, we have for the first time implemented a single point of contact for cybersecurity within the Federal Government that will interact with other agencies, private security, the resource communities and State and local governments on a 24x7 basis.

Third, though the director of the NCSD serves as a technical and operational lead for cybersecurity issues, cybersecurity will also be championed by Under Secretary Frank Libutti and myself. And we are committed to the implementation and the full funding of the NCSD as one of the top priorities for the IAIP directorate and for DHS at large.

As demonstrated by recent events, the consequences of cyber attack can manifest with little or no warning, on a widespread scale, with tremendous speed. Impacts can quickly escalate across multiple infrastructures, resulting in widespread disruption of essential services, significant economic losses, and potentially endangering public safety and national security. The NCSD, therefore, is implementing its objectives for the timely execution of three key mission areas—outreach, prevention, and remediation.

The NCSD is aggressively pursuing an outreach agenda that will provide education tools for children, parents, teachers, business owners, and business operators. NCSD, through the development of partnerships with government agencies such as the Federal Trade Commission, nonprofits like the National Cybersecurity Alliance and Internet service providers, will work to establish and enhance awareness programs for all users at all levels. We will be making announcements on our progress in the coming weeks.

NCSD partnerships with industry, academia, and government will be the foundation for program implementation for protective and preventive measures to reduce America's vulnerabilities to cyber attacks. It is crucial that we improve existing public and private partnerships whose missions are consistent with the NCSD.

A prime example is the National Cybersecurity Alliance whose members have committed their time and resources to regularly educating the home consumer and small businesses on good security practices. Proactive response and recovery efforts associated with the recent Blaster worm and SoBig virus offer the best evidence of the value of partnerships. SoBig spread faster and more aggressively than any previous e-mail virus, affecting millions of residential business and government computers worldwide.

We recognize a cyber attack could easily cascade across multiple infrastructures, causing widespread, rapid disruption of essential services and impacting our national economy, public safety, and national security. The NCSD is committed to closely working with other government and law enforcement agencies, private industry, as well as academia, to help secure our cyberspace from future and potentially more serious malicious exploitation.

To this end, I am pleased to announce that we are beginning to organize a National Cybersecurity Summit for later this fall in order to assemble key industry and government leaders to energize decisions like several key national cybersecurity issues.

The Internet and cyber technologies have greatly improved both the quality of life for our citizens and the efficiency and the productivity of our business and our government. These societal and economic benefits are not without their costs. Malicious actors are devising new and ingenious ways to exploit vulnerabilities in our cyber world, to disrupt our quality of life, and threaten our national and economic security. Much like the larger global war on terrorism, this effort will take time, resources, dedication, energy, and hard work. But in the few short months we have been in existence, we have made great strides and we look forward to working with the Members of Congress, this committee, our government partners, the private sector, and the international community in this endeavor.

I come before you today to dedicate ourselves to this common goal: one team, one fight, one mission, to protect the United States of America.

I appreciate the opportunity to testify before you today and I look forward to your questions. Thank you.

[The statement of Mr. Liscouski follows:]

PREPARED STATEMENT OF THE HON. ROBERT LISCOUSKI

Good morning Chairman Thornberry and Members of the committee. My name is Robert Liscouski, I am the Assistant Secretary for Infrastructure Protection and Acting Director of the National Cyber Security Division (NCSD) within the Department of Homeland Security. I am pleased to appear before your Subcommittee to discuss some of our efforts to protect and secure our Nation's critical infrastructure.

Last week's observances of the two-year anniversary of the September 11th attacks offer a stark reminder of the threats and vulnerabilities we as a Nation still confront. The Department's Information Analysis and Infrastructure Protection Directorate (IAIP) was established by the Homeland Security Act to lead the Nation's efforts to prepare for, prevent, respond to, and recover from terrorist attacks like those perpetrated on 9/11. These terrorist acts may manifest in many forms, including physical and cyber attacks against our critical infrastructure, key assets, and national icons. Both physical and cyber assets have vulnerabilities that may be exploited by our enemies. The highly interconnected nature of our infrastructure makes these physical and cyber weaknesses impossible to separate—and difficult to address separately. Our protection methodology leverages an integrated physical/cyber protection approach to reduce vulnerabilities and to optimize our response when an attack does occur.

From the beginning of DHS, the IAIP directorate which includes the Infrastructure Protection Office for which I am responsible, has implemented a dedicated organization committed to protecting physical assets. The organization is called the Protective Security Division (PSD). Recognizing the equal importance of protecting cyber assets, we created the National Cyber Security Division on June 6 of this year. These organizations within the Infrastructure Protection Office work together to implement the integrated protection methodology that I previously discussed. Today, I am here to give you a progress report on where we are now, and what we have in store for the coming months and years to implement the President's National Strategy to Secure Cyberspace.

I am pleased to announce that Amit Yoran has been formally named as the Director of the NCSD effective today. Mr. Yoran is a strategic, disciplined leader who understands the unique threats and vulnerabilities manifested in cyberspace and is an individual capable of managing a diverse, highly technical organization Mr.Yoran was most recently the Vice President for Managed Security Services at Symantec Corporation where he was primarily responsible for managing security infrastructures in 40 different countries. Before working with Symantec, Mr. Yoran was the Founder, President and CEO of Riptech, Inc., a leader in outsourced information security management and monitoring. Before working in the private sector, he was the Director of the Vulnerability Assessment Program within the Computer Emergency Response Team at the Department of Defense and the Network Security Manager and the Department of Defense where he was responsible for maintaining operations of the Pentagon's network Mr. Yoran's leadership and respect within the information security industry will further accelerate our efforts in building the full NCSD team, and increasing the strength of our public and private sector partnerships.

Since its formal establishment in June, the National Cyber Security Division has worked closely with our partners in the private sector, including coordinating response and mitigation of the Blaster worm and SoBig virus. Without these coordinated efforts, the significant economic impact of these attacks could have been much worse. In each situation, the Department's cyber security experts demonstrated the ability to quickly reach out to the security community, rapidly assess emerging threats, and provide timely warnings to government, industry, and the general public. These initial efforts were crucial—they allowed the NCSD to establish its credibility and demonstrate its value to the national and international cyber security community.

Since June, IAIP has been assembling a consolidated and coordinated team of cyber security professionals. These experts were integrated from portions of the National Infrastructure Protection Center (NIPC), Critical Infrastructure Assurance Office (CIAO), Energy Assurance Office (EAO), and the Federal Computer Incident Response Center (FedCIRC). Despite the many organizational and cultural challenges associated with integrating these elements into one entity, our initial efforts have yielded effective and tangible results. Creation of the NCSD has enabled:

- Planning for consolidation of three 24x7 cyber watch centers;
- Formulation of a standardized incident handling procedure for responding to cybersecurity events; and
- Creation of a single national focal point for cybersecurity leadership for prevention, protection, and response to incidents.

The most recent accomplishment of the NCSD is the creation of the National Computer Emergency Response Team (US-CERT). The US-CERT, in collaboration with the private sector and leading response organizations, will improve warning and response time to security incidents by fostering the development of detection tools and utilizing common commercial incident and vulnerability reporting protocols. This will increase the flow of critical security information throughout the Internet community by leveraging the extensive resources and brand of the Federal Government and Carnegie Mellon's CERT/Coordination Center. The CERT®/CC is a part of the Software Engineering Institute (SEI) and is affiliated with Carnegie Mellon's new Cyber Security Laboratory. A key enabler of this partnership is the 19 years of leadership demonstrated by the U.S. Department of Defense in its sponsorship of the SEI, a federally funded research & development center. By integrating capabilities from the Government (FedCIRC), Academia (The CERT®/CC), and the private sector (vendors of security products and services), the US-CERT will provide a coordination center that, for the first time, links public and private response capabilities to facilitate communication across all infrastructure sectors.

Before detailing our future programs and initiatives, I would like to begin by providing rationale behind the decision to treat physical and cyber security on part with one another, within the IAIP directorate. I believe that this approach is the correct one for three reasons.

First, cyber security cannot be a "stand alone" effort. As I described earlier in my statement, the success of DHS as a Department, and IAIP specifically, depends on our ability to protect the entire critical infrastructure against physical and cyber attacks *together*. We realize the dominant components common to all 13 critical infrastructures are physical and cyber components. To best protect the country against attack, careful integration of both components is required to achieve a holistic view of critical infrastructure vulnerabilities. In fact, this view is validated by a common criticism voiced by the private sector and security experts preceding the creation of the Department: physical and cyber security were being addressed by the govern-

ment independently. We believe the physical and cyber domains are inextricably linked and vulnerabilities cannot be effectively analyzed independently. Placing both responsibilities under one Under Secretary and one Assistant Secretary has ensured successful integration.

Second, the NCSD will identify, analyze, and reduce cyber threats and vulnerabilities; disseminate threat warning information, coordinate incident response; and provide technical assistance in Continuity of operations and recovery planning. With the creation of the NCSD, we have for the first time, implemented a single point of contact for the prevention, protection, and coordination of response to incidents, that will interact with all federal agencies, private industry, the research community, State and local governments, and other partners on a 24x7 basis.

Third, while the Director of the NCSD serves as the technical and operational lead for cybersecurity issues, it is important to remember that the cyber security issue will now be championed within IAIP by Under Secretary Frank Libutti, and myself. The Under Secretary and I have already demonstrated our commitment to developing a world-class cyber security capability within the Department and believe the continued implementation and full funding of the NCSD is one of the top priorities for the IAIP Directorate. Furthermore, cyber security research and development will be conducted in partnership with the Department's Science and technology Directorate under the leadership of Under Secretary Charles McQueary.

Now I would like to focus the remainder of my testimony on our plans for building on our accomplishments of the last three months to fully implement the operational NCSD in the coming months.

The Mission: Outreach, Prevention, and Remediation

As demonstrated by recent events, the consequences of a cyber attack can manifest with little or no warning, on a widespread scale, and with tremendous speed. Impacts can quickly cascade across multiple infrastructures, resulting in widespread disruptions of essential services, significant economic losses, and potentially endangering public safety and national security. The National Cyber Security Division, therefore, is implementing its objectives through the timely execution of three key mission areas—Outreach, Prevention, and Remediation.

Outreach

The NCSD will create, in coordination with the Office of Personnel Management and the National Institute of Standards and Technology, cyber security awareness and education programs and partnerships with consumers, businesses, governments, academia and international communities.

An effective outreach program lays the foundation for the ultimate success of all mission areas of the NCSD. Accordingly, the NCSD championing the implementation of awareness efforts and campaigns that use a multi-level approach to provide awareness/educational tools for all users; for the home, awareness tools for children, parents and teens; customized approaches for small, medium, and large businesses; and for government agencies. Every level of user must realize they have an equally important role in the security of cyberspace. The end user, for example, needs to be informed about the technical aspects of security and about their role as gatekeepers in a larger data and information sharing community.

The NCSD is aggressively pursuing an outreach agenda that will target groups of citizens by providing education tools for children, parents, teachers and business owners and operators. There are many effective existing programs and the NCSD is developing partnerships with government agencies, such as the Federal Trade Commission, non-profits like the National Cyber Security Alliance, and the Internet Service Providers to establish and enhance awareness programs for all users. We are working to build on existing public/private outreach groups to assist the spectrum of users in securing their systems through implementation of effective security practices.

One quick example is establishing National Cyber Security Days. As Americans change their clocks twice a year, to Daylight Savings and Standard times, the partnership of the NCSD and the National Cyber Security Alliance's StaySafeOnline Campaign asks consumers to use the days as reminders to assess their own computer security. Computer security needs to be a regular consideration when protecting a home. Just as consumers remember to lock their doors, so too should they remember to secure their computers. As a result of this partnership with the NCSD many other partners in the business and government communities are starting to design their national ad campaigns around these two dates to further amplify this important message.

At the same time, the NCSD is partnering with other federal agencies, including, Commerce, NSA and DOD, state and local government, private industry, and academia to promote a well-trained IT security workforce.

Prevention

Consistent with law and policy, NCSD will coordinate closely with the Office of Management and Budget and NIST regarding the security of Federal systems and coordinate with Federal law enforcement authorities, as appropriate. NCSD will leverage other DHS components including the Science and Technology Directorate, the U.S. Secret Service and the Department's privacy officer.

To achieve its mission, the NCSD is working with State and local governments, and the private sector to conduct infrastructure vulnerability field assessments, while providing the best and most cost-effective prevention and protection strategies for "at risk" infrastructure facilities, assets, and personnel. Due to the diversity of the critical infrastructure, cyber protection strategies for each sector must be customized based on the unique geographical and business operating models of that sector. Due to the highly interconnected yet physically distributed nature of our critical infrastructure, prevention and protection strategies are prioritized based on regional, State, and local needs and on the need for cross-sector coordination.

We recognize that collaborating with industry, academia, and Government is a key focus of our NCSD activities. With partnerships as the foundation for program implementation, the NCSD will coordinate implementation of protective and preventative measures to reduce America's vulnerability to cyber attacks. It is crucial that we improve existing public-private partnerships whose missions are consistent with NCSD functions. A prime example is the National Cyber Security Alliance, whose members have committed their time and resources to regularly educating the home consumer and small businesses on good security practices.

With nearly all of the backbone of cyberspace owned by the private sector, it is imperative that the NCSD strengthen its relationships with them. Fortunately, there are mechanisms already in place to facilitate cooperation between industry and government on cyber security, most notably the National Coordinating Center (NCC) for Telecommunications and its Telecommunications Information Sharing and Analysis Center (ISAC), which are each part of the National Communications System (NCS) and IAIP. These entities provide the Department with direct access to leading industry operational and security experts whose knowledge and insights may prove crucial in managing a cyber incident. The NCSD, as part of IAIP, also helps to support two CEO-level advisory committees—The National Security Telecommunications Advisory Committee (NSTAC) and the National Infrastructure Advisory Council (NIAC),—which provide advice and counsel on national security telecommunications and critical infrastructure matters, including cyber security issues.

By acting as a champion for creating a national and international culture of cyber security, we aim to promote a security culture at the CEO-level and demonstrate to corporate leaders that cyber security ultimately promotes the resiliency of their infrastructures, protects the interests of their shareholders and corporate brand, and preserves value and competitive advantage for businesses that implement security best practices.

Remediation

As I discussed earlier, the proactive response and recovery efforts associated with the Blaster worm and SoBig computer virus offer the best evidence of the value of partnerships. SoBig spread faster and more aggressively than any previous email virus, affecting millions of residential, business, and government computers worldwide. Internet traffic was substantially affected by these two events, causing a 25 percent increase in internet traffic and infecting over 600,000 computers. It had a significant impact on cross-sector communication and impacted productivity.

In August, when the Blaster worm surfaced on the Internet, the NCSD issued a timely warning to security professionals, suggesting that Internet service providers and other corporate network administrators shut off inbound traffic to ports 135, 139, and 445 to block the spreading of the Blaster infection. Blaster took advantage of a known vulnerability in a Windows operating system component that handles messages sent using the remote procedure call (RPC) protocol. RPC is a common protocol that software programs use to request services from other programs running on servers in a networked environment. Vulnerable systems were compromised automatically without any interaction from users. Through the advisory, users were instructed to install the appropriate software patches to prevent their computers from being infected. In the following weeks, the NCSD continued to issue advisories warning security professionals that a variant of the Blaster worm, dubbed "nachi," "welchia" or "msblast.D," was proliferating.

Working with Internet security researchers and experts from private industry and academia, the Division and the FBI uncovered malicious code hidden within the SoBig worm on twenty master machines that was programmed to launch a massive denial of service attack. Federal authorities located the twenty computers infected

with this variant of the worm and asked their Internet service providers to shut down their Internet access. As a consequence, the second wave of attacks never materialized.

The NCSD recognizes that a cyber attack could cascade across multiple infrastructures, causing widespread rapid disruption of essential services, and impacting our national economy, public safety, and national security. While this generation of worms has not yet resulted in irreversible damage (albeit slowing communication, overstuffing e-mail inboxes, and reducing productivity), the NCSD is committed to working closely with other government and law enforcement agencies, private industry, as well as academia to help secure our cyberspace from future, and potentially more serious malicious exploitation.

To this end, I am pleased to announce that we are beginning to organize a National Cyber Security Summit for later this fall, in order to assemble key industry and government leaders to energize decisions on several key National cyber security issues. Key goals of the summit are to—.

- Produce a common threat and vulnerability reporting protocol to enhance prevention and response capabilities and to drive a standards-based system for communicating threats and vulnerabilities across the Nation;
- Develop a Vulnerability Reduction Initiative to significantly reduce vulnerabilities based upon improved evaluation standards, tools and measures for software, new tools and methods for rapid patch deployment, and best practice adoption of security for cyber systems across the critical infrastructure in partnership with industry and the leading research universities in the United States;
- Create an outreach and education partnership to offer training and awareness to 50 million home users and small businesses in cyber security within one year; and
- Formulate and ratify a National Cyber Security Road Map that defines milestones, work streams, and metrics for "raising the bar" of cyber security across the United States and identify work stream leads from government and industry.

Since its inception, the National Cyber Security Division has delivered on its commitment to provide a centralized coordination point for the collection and dissemination of protective measures to reduce vulnerabilities and risks to the cyber infrastructure through implementation of the Cyber Security Tracking Analysis and Response Center (CSTARC). As announced in our press release on Monday morning, CSTARC, through a partnership with Carnegie Mellon University's CERT®/Coordination Center, will evolve to a new capacity as a national Computer Emergency Response Team (US-CERT). The US-CERT will enhance our Nation's prevention of and response to cyber threats and vulnerabilities. There are currently over two hundred private sector groups, public sector groups, and universities that operate computer emergency response teams (CERTs) within the United States. Many of these groups have varying levels of informal and formal partnerships with each other and with the US-CERT. This initiative will harness this massive capability to significantly increase America's ability to protect against, and respond to, massive scale cyber attacks.

We view the US-CERT as a fundamental element of the DHS strategy to ensure timely notification of all types of attacks, working toward having, within a year, an average of a 30-minute response to any attack. Moreover, the US-CERT will provide a coordination center that, for the first time, links all public and private response capabilities and facilitates communication across all sectors. US-CERT will also lead collaboration with the private sector to develop and distribute new tools and methods for detecting and identifying vulnerabilities in an effort to significantly reduce vulnerabilities. Lastly, US-CERT will help improve incident prevention methods and technologies by identifying and disseminating best practices and working with the private security industry to improve warning sensor data collection and analysis.

Conclusion

The Internet and cyber technologies have greatly improved both the quality of life for our citizens and the efficiency and productivity of our businesses and our government. These societal and economic benefits are not without their costs. Malicious actors are devising new and ingenious ways to exploit vulnerabilities in those cyber systems, to disrupt our quality of life and to threaten our national and economic security. Our ever-growing reliance on the Internet and cyber systems compels us to counter these threats and vulnerabilities by building productive partnerships with key stakeholder communities in cyberspace, improving how we share information, and developing and fielding innovative technical solutions. As the focal point for the prevention, protection and coordination of response to incidents, the NCSD

must achieve its mission of ensuring the security of cyberspace. We know this will not be an easy assignment. Much like the larger global war on terrorism, this effort will take time, resources, dedication, energy, and hard work to succeed. But in a few short months, we have made great strides and are excited about the possibilities that the future offers. With the appointment of the new Director of the NCSD, we have focused leadership to guide us forward, to forge new alliances and partnerships, to implement new tools and capabilities, and to provide a vision for cyberspace security.

Again, I appreciate the opportunity to testify before you today. I would be pleased to answer any questions that you have at this time.

Mr. THORNBERRY. Thank you. And I can assure you that this subcommittee shares your goal of working together to help the country be safer. Let me just ask one brief question before yielding to Ms. Lofgren.

It seems as though that the Department has made several significant announcements yesterday and today. The establishment of the US–CERT, the naming of the Director for the Cybersecurity Division, and now this National Cybersecurity Summit, which will take place later this fall.

Why is it all coming down now? What has been your decision-making process, and why are we just having these decisions made.

Mr. LISCOUSKI. Well, Mr. Chairman, it is a function of our timing is, we have been working very hard since June, and as you well know, we have engaged in a lot of other activities in standing up the division.

One of the things I have been working hard at over the past few months is putting the right team in place to ensure we could actually carry out the things that we announced just these past couple of days. So it is one.

We could have announced them, or at least our intention is to execute on these objectives, earlier; but the framework from which we are operating is really one in which we plan carefully, but quickly, and then with the ability to execute.

So I am here before you today to say that our announcements are timed with our ability to execute, not so much as anything else, but just a function of the ability that we are working very hard, and we have got a good plan together, and we finally have our teams together to be able to execute on the strategies we have identified.

Mr. THORNBERRY. Yield to Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chairman. I have just a few questions.

As I mentioned in my opening statement, the President had a Special Advisor on Cybersecurity, but that position has been eliminated. Will the director of the Cybersecurity Division have direct contact with the President or with Secretary Ridge on cybersecurity issues? What kind of access will this individual have?

This is kind of a nerdy subject we all know that and yet it is very important; and it is important that the decision makers, who are not necessarily living and breathing computer, be contacted and be aware of the scope of the issues.

Mr. LISCOUSKI. Yes, ma'am. Mr. Yoran—first of all let me explain.

Our management style at DHS is, one, a very direct one. Working for Under Secretary Libutti and Secretary Ridge requires one to be constantly engaged to ensure that the leadership knows what is going on. I mean, this is a constant dialogue we have at senior

management levels, particularly as it relates to infrastructure protection. Information analysis, because of the very uniqueness of what IAIP brings to the Department in terms of a function, is one which is heavily relied upon by the senior management of DHS. So I can tell you from personal experience that Secretary Ridge, Under Secretary Libutti reach down into the organization at any level that they think they need to get the answers to questions that they have, and we are very responsive.

To that end, Secretary Ridge has been personally involved in not just overseeing the implementation or the creation of this division, but engaged with me in identifying the type of leadership we need and what we need to do to be successful in this endeavor. So if Mr. Yoran is going to have the the pleasure, because it is indeed a pleasure to work with the senior leadership, but more importantly the responsibility of reporting directly. My management style, Under Secretary Libutti's management style, is not one in which we say, You have got to go through a, quote, unquote, "chain of command." Ours is pretty much, You are the expert, you have got the con, you take the lead, answer the questions, take the initiatives.

Ms. LOFGREN. Okay. That is very reassuring. Thank you.

One of the questions I was mentioning to the chairman, there is modeling going on around the country, university based, and I am interested in whether the Cybersecurity Division will be working with the Science and Technology Directorate on modeling in simulation issues and whether cyber threats are going to be integrated into these efforts. Can you give us a progress update on that?

Mr. LISCOUSKI. Yes, ma'am. Let me take the partnership with S&T first because I think that is where it starts.

The Cyber Division has got a direct nexus into Under Secretary McCrery's S&T organization, the Directorate. We have a deputy director named in the research center in S&T. So we are directly partnering by driving requirements in S&T that we have identified from the field, not just from our own efforts, but through our partnerships with State and local governments, with the industry, with our international partners. We are taking those requirements and driving them into S&T. That is point number one.

As it relates to the universities, our relationship with the US–CERT at Carnegie Mellon clearly is one example. We have many other relationships with universities and labs to do modeling. We have got the benefit of having the opportunity of reaching out to lab relationships we have currently that came over to us when we formed DHS earlier this year, so we have already been working on computer simulations for different types of modeling for attacks and for things that relate to cybersecurity as well as other parts of our infrastructure.

Ms. LOFGREN. Can I ask you about this US–CERT? I saw the announcement. We have the Federal Government has been a partner with CERT at Carnegie Mellon for many years. And how is US–CERT going to be different than regular old CERT?

Mr. LISCOUSKI. Well, I would like to recognize the Department of Defense obviously for taking the initiative back some almost 20 years ago, after the Morris worm, to establish the CERT/CC capa-

bility. That relationship has allowed many parts of the Federal Government to take advantage of the CERT capabilities.

CERT, as you well know, remains one of the premier capabilities in the world, and to that end, the partnership that DHS is establishing is a key one for us because we are increasing our level of financing to the CERT. So therefore we are increasing the resources available directly to DHS, vis-à-vis the CERT, to do things not just around the incident response area, but also looking at establishing a malicious code lab there, as well as other enhancements through financing, through partnerships, through positioning people at the CERT, working closely with them to ensure that US–CERT can mature to a capability that is going to serve the National Strategy for Cyberspace.

Ms. LOFGREN. Finally, one of the responsibilities of your office is to coordinate outreach to State and local governments, and I am interested in how you are doing that. Is there an office that is responsible for outreach? Is outreach institutionalized? And in particular I am interested not just in what we might think of as cybersecurity, but the physical infrastructure that allows the cyber world to exist; and I continue to be concerned about the level of information and coordination between the Federal Government and State and local, especially local police officials, in terms of vulnerabilities that exist to the physical infrastructure.

Because we are very concerned with the viruses and worms and cyber attack, but the model for terrorists remains some maniac with a bomb; and so we have vulnerabilities in that area that I am not yet convinced we have addressed adequately. And really our first line of defense is going to be local, not Federal officers.

So can you address that issue for me?

Mr. LISCOUSKI. Yes, ma'am. And I agree with you; I don't think we have addressed it adequately yet either. We are working hard to do that. We have got a number of mechanisms for outreach, and let me just articulate those.

We have a branch in the NCSD dedicated to outreach. It is headed up by a very seasoned professional. Sally McDonald, who came to us from the Fed CERT, has done a tremendous amount of effort in outreach and has got a lot of experience in this area, so we are relying upon Ms. McDonald to really take the programs where we need to go.

We have a number of programs currently established at the NCSD. StaySafeOnline Campaign is one of the dominant ones in which we are using that to reach many different levels of constituents in the cyber world. That is just one example.

We are partnering up as you may know, we have got relationships with ISACS, the Information Sharing Analysis Centers. There is an IT ISAC, but there is a cyber component in every ISAC we use for outreach.

We have our advisory systems in which we put out notices about threats or incidents and events relating to the cyber world.

We are going to continue to use the private sector for outreach. Our partnerships with the private sector are absolutely key for us to ensure that we have got the right things, the right awareness, going on because, as you are fully aware, this problem is not necessarily just a technological problem. In fact, most computer secu-

rity professionals would articulate that the problem is typically not the technology; it is the implementation of proper standards and procedures to ensure that the technology is used accordingly, patches are made, remediation work is being done. And those are process issues; those are not technological issues.

It is all about awareness training, so we are reaching out using universities, using the private sector, using our own outreach capabilities to ensure we have multilevel awareness programs going on; and these are in development, and we are welcoming suggestions from any of those out there, anybody who has got an interest in this area to ensure we are doing the right thing.

As I mentioned in my statement, we are working with ISPs to ensure that we have got the right awareness going on for users of broadband connections to ensure that they understand the dangers of getting on line and in open systems without taking the appropriate precautions, so—.

Ms. LOFGREN. Thank you. I will reserve my other questions for the next second round.

Mr. LISCOUSKI. Thank you.

Mr. THORNBERRY. I think the Chair will use the clock not just as a guide for members, not as a hard and fast rule; and Ms. Lofgren and I have agreed that we will have as many rounds as members have questions, with Mr. Liscouski's indulgence.

The Chair would now recognize the gentlelady from Washington.

Ms. DUNN. I thank the chairman.

Mr. Liscouski, this committee has made it a priority to understand how communications and information are being shared across Federal agencies. How will the Cyber Division work within the larger Information Analysis Division responsible for analysis and warnings to the Homeland Security community and, if necessary in an extreme case, to the public?

Mr. LISCOUSKI. Let me describe first our relationship with the Information Analysis Office. That is the IA component of IAIP. We are tightly knit together. The IAIP Directorate, combined of those two offices, was created with the intention of ensuring that we had overlap of our functions and our thinking within the structure to ensure that we always had a very close look at the intelligence components of the threats mapping vulnerabilities, whether they be physical vulnerabilities or logical or cyber vulnerabilities.

And in this case, the NCSD plays sort of a unique role. While it is not an intelligence function, it is a capability-oriented, technical capability. And we lend ourselves to the IA function to understand how technical exploits can be used to conduct cyber terrorist attacks, while the IA function has clearly got the intelligence requirements to understand how terrorist groups may, or what their intentions may be to use technologies to conduct a cyber attack. They are a portal to the Intelligence Community.

We drive our requirements through the information analysis component to ensure that they maintain that constant look and their constant contextual piece around what we are worried about from a vulnerability standpoint and what the Intelligence Community needs to be looking at from an intelligence standpoint. So we are tightly integrated. We drive requirements. We have—the IA analysts are frequently as knowledgeable about the technology, at

least at a top level, as our folks are to understand what the vulnerabilities are. So when they see intelligence pieces they understand the relevance of intelligence to a particular infrastructure component.

Ms. DUNN. Will you find yourself working with TTIC, with or through TTIC, during any of the process?

Mr. LISCOUSKI. Yes, ma'am. We would be working with TTIC, and we do now quite actively through our IA counterparts; and my colleague, Bill Parrish, the Acting Assistant Secretary for Information Analysis can go into that much more deeply. But I am very familiar with our relationships there. We use them quite robustly.

But, again, we drive those through the IA component, ma'am.

Ms. DUNN. Do you—in your Cyber Division, do you believe now you have adequate resources to conduct all your activities? Are there areas where you see specific needs our committee ought to be focusing on?

Mr. LISCOUSKI. I think, for the present, we have the resources we need. As you know, we are staffing up. We currently have approximately 65 people in the division, and we are looking to staff up to somewhere, I would say about 100 or so for fiscal year 2004 is our plan.

From my perspective, I think we are adequately staffed. I think we have got the resources we need, particularly with the partnership with the US–CERT. I think downstream, as we learn more about the vulnerabilities and particularly the initiatives we want to take and the resource areas in the short terms areas that we need to make improvements, we will probably be coming back to this committee and articulating what those needs are.

Ms. DUNN. I am not seeing any timing clock. Do you have one, Mr. Chairman?

Mr. THORNBERRY. The green light is down in front of the witness.

Ms. DUNN. Got it.

As I mentioned in my opening statement, we all fully appreciate cyberspace has no borders. How will you find yourself working with international organizations in your role?

Mr. LISCOUSKI. The international component is a very critical one for us. As you know, we have some informal arrangements. We are working closely with the British Government, with the Australians, the Germans, the Canadians.

It is critical for us to expand our relationships for international cooperation. We are working with the Department of State to formalize those agreements. Bilateral and multilateral agreements are very key for us.

The national strategy articulated the need for signing for the—I am sorry—the European convention on cybersecurity. That is not the exact term, but we fully support that.

We need to work with the international community to ensure that we have got uniform laws across international boundaries to enforce violations, to ensure that we have got good thinking about best practices.

To your point, there are no boundaries. A vulnerability in Slovakia is as critical as a vulnerability in the United States. If a company is a Fortune 50 company operating around the world, we have

to be very cognizant of those vulnerabilities. We are working hard with our partners to bring them up a level of capability, as well.

Ms. DUNN. And does that include cooperative working when responding to something?

Mr. LISCOUSKI. Yes, ma'am. The US–CERT is going to be nexus for that capability. We are going to be using the US–CERT as a model for CERTs around the world to—and this has clearly been the model.

So to your point, yes.

Ms. DUNN. What about—is your division considering and in cooperation with the private sector, considering setting up a code of standards, best practices, that would be in place both for the private sector, which you, in your testimony, mentioned had something over 80 percent of all of the cyber work that we need to be dealing with and also the public sector?

Mr. LISCOUSKI. Yes, ma'am. And best practices occur at many different levels.

We are trying to articulate identify and articulate best practices for home users, for small businesses, universities, big businesses. We have got to work in cooperation with the industry to ensure that best practices are effective, implementable, cost-effective, measurable, all the elements that you would want to have programs to identify what the right level of security is.

This is a big area, a big body of work, and we are spending, we have been spending time, and we are spending much more a lot more time in the future on this. We are working with our councils. We have got the NIAC, the National Infrastructure Advisory Council, you are familiar with, I am sure; the NSTAC, the National Security Telecommunications Advisory Council. Both of those bodies have been involved in helping us identify standards.

We are working with the private sector to determine what additional standards may be necessary. We are going to make these standards publicly available on our Web sites as we promulgate them. So this is all part of our outreach program.

Ms. DUNN. And you can do that, you believe, without legislation?

Mr. LISCOUSKI. Yes, ma'am. And I think at this point in time, we have got the industry with the support of the Congress, with the support of this administration, attuned to the need that security is more than just something which you can spend a dollar for and say, I have got adequate security.

The biggest challenge in the business community is, again, ensuring you can identify what the appropriate level is and what the right level of investment for a dollar of security, does it get you anything in return. The cost and the return on investment is always a key component in the private sector.

The business case here in terms of why businesses should be spending money on security in advance of legislation, I think, is one which is based upon competitive advantage. The more we can educate consumers, either at the basic consumer level, those who might shop at Amazon.com on line or those who implement multimillion dollar programs in their businesses, should know that they have choices about what the right choices are to make for security, for levels of security in the technology that they are buying; and the more we can make those—that awareness known to the con-

sumer groups, the more pressure they will put on the private sector to ensure that security is baked into their programs.

Ms. DUNN. Good. Thank you very much.

Thanks, Mr. Chairman.

Mr. LISCOUSKI. Thank you.

Mr. THORNBERRY. Thank the gentlelady. The gentleman from North Carolina.

Mr. ETHERIDGE. Thank you, Mr. Chairman, and thank you for holding this hearing. I think it is we all know how important it is.

Mr. Liscouski, when we think in terms of cybersecurity, a lot of folks, when they first hear it, they think of it as how we protect computers. The truth is, as you know, it is much broader than that, because so much of our productivity and our economic fiber of this country is tied to the whole integration system that we have; and over the last 10, 20 years we have seen tremendous amounts.

So let me get back to the risk assessment, and I am going to try not to cover something that hasn't been covered, but maybe get a little better perspective on it. Because realizing that a department is just gearing up, and thinking about just the amount of problems we have had that was mentioned by our ranking member just this past August, the economic damage that was done to business and others by independent assessments, by some of the digital risk companies are saying it was about $32 to $33 billion. So obviously, this whole issue of cybersecurity is a huge issue.

What progress has the Department of Homeland Security made in identifying cyber threats and vulnerabilities? And in conjunction with that, how have you been able to share this information with State and local organizations, which I think is critical? You know, just because they have the information doesn't really do us a whole lot of good unless we can figure out how we can get it, to get some results in the assessment area.

Mr. LISCOUSKI. It is an excellent question because it is the heart of what a good protection program is all about: understanding the risks, the vulnerabilities to those risks, and the right practices in which you can engage to mitigate or reduce those risks or alleviate them.

To that end, a major component of what we have done there are a number of them. We have got one effort as part of our responsibility for securing the Federal Government, which is initiated through the Fed CERT. That is the responsibility, to ensure that the proper warning alerts, incident notices, are going out across the Federal Government.

That program has been in place for a while, originally established with GSA, now moved over to DHS, and is, at the heart, the NCSD. It is a very robust program. Part of that is also a patch remediation capability which goes back to the reduction of vulnerabilities and spreading that word.

As it relates to the private sector and State and local governments, I think that is where much of our work is required to be done yet. We have got great relationships in the private sector in providing us information about vulnerabilities. Our relationships with Microsoft, with Cisco recently, have enabled us to be able to respond very quickly to vulnerability information and exploits and put notices out there to the general public and the State and local

governments as well. They are all on the same alert system, so therefore they have the opportunity of receiving this information very quickly.

It is our goal, with the establishment of the US–CERT and the leadership that we are establishing in the NCSD, to reduce these notification times from hours, currently, to, hopefully by the end of fiscal year 2004, an average of 30 minutes. We are looking to get robust communications capabilities out there beyond what we have now working, establishing networks with State and local governments.

We have got some efforts under way right now, which I would like to keep at a top level, in terms of working very closely with State initiatives to develop communication networks, and then ultimately to establish State CERTs again, using the US–CERT as a model to reach down into the State governments to help them set up their own capabilities for incident response and incident warnings.

So there are a number of initiatives we have got going in the pipeline. Again, we have only been working here for 3 months, so we are moving from the thinking and planning stages into the execution stages in the next quarter.

Mr. ETHERIDGE. Let me follow that up, if I might, please, because I think you moved into the advisory and warning area, which I think is very critical as you deal with the assessed risk assessment.

You have started a long—but as the Department looks at this whole area of integrating warnings about the possible problems of cybersecurity, and you have talked about what you are doing across the Federal Government to get it done on the security advisory system, talk to us a little bit more, if you will, please, about how are you reaching out to locals. You have talked about it in general terms. Because I think it is important, because most of the people who are going to be called upon to respond to such an attack are not traditional first responders, as we think, in terms of the agency reaching out to first responders—our fire, police or rescue; they are important because they have to receive it too—but you are also talking about a whole new group of first responders.

How about talking about how those two are integrated, because I think it is critical to know, and what the Department is doing on it? Because if all you do is go to the end user, that will help, but you have really got to get upstream; and I hope that is what you are talking about.

Mr. LISCOUSKI. Yes, sir. And if I understand your question correctly, this is again a multilevel approach.

Mr. ETHRIDGE. Absolutely, because you have also got the private sector category there.

Mr. LISCOUSKI. That is correct.

The first responder category in the cyber world is every user. I mean, it starts with prevention, as you well know, and ensuring we have got the right procedures in place to protect our systems; and that is just through basic security practices.

Part of our outreach program is intended to continue to elevate the level of awareness and understanding and security posture within our—across the entire Nation by getting the average user or the business user to understand what they must do to protect

themselves. In response mode, I think the Blaster and the SoBig virus are a example of how our response needs to be enhanced. I think we did a very admirable job responding and putting the advisories out, and we got a significant reach across our community to do that, both horizontally and vertically within the State and local government community, as well as in the private sector.

But the home user was the one that I believe probably lacked the ability to understand what the implication of the—they clearly understood the implication, primarily because they couldn't get on the Internet. It was—remediating from that problem was where we saw the biggest challenge to be.

So we are looking at many creative ways to put out the word. We are working with the major media, establishing relationships with the major media to put the word out to make sure we have got a consistent message across there. Information sharing is the primary goal of DHS.

It is often said, you know, it is not need to know, but it is need to share, and we are looking for as many ways as we can to put the information out there—on best practices, on vulnerabilities, on threats—that we possibly can, irrespective of whether they are in the physical world or the cyber world. We are not differentiating those things.

The only thing I would add, and I can probably get into this a little bit later, is the speed at which the cyber world works. As you well know, it requires a little bit of a different sort of ops tempo, so to speak, or posture in ensuring that we have got a consistent, a thorough and a consistent look across all the infrastructure to ensure that we are aware of what is going on in the cyber world.

I can address that later.

Mr. ETHRIDGE. Mr. Chairman, I know my time is up, but may I follow up with one final, since we are on this point, because I think it is so critical as we do this.

I hope at some point we have in the system a measurement to know at least when we have we have had some measure of success. You know, it is one thing to do the assessment, another to notify. But unless we have a measurement down the road we talk about what business does in terms of measuring inputs and outputs. But we have to find a way to know, because this pressures us to speed up our process in the decision-making process to save those multitudes of billions of dollars down the road.

Mr. LISCOUSKI. You are absolutely right, sir. It is about metrics. It is about ensuring we can find those measurable programs and those factors within our programs to determine if, in fact, we are doing the right thing. That is precisely the business approach that we are taking.

Again, going back to the leadership—and the comments earlier, ma'am, about, you know, why it took so long to find our director—the only response on that is, we wanted to make sure—we are only going to get a chance of doing this right once, and finding the person with the right capabilities and qualifications that can understand working in an entrepreneurial environment.

How do you build an organization and who do you be able to quickly execute against the requirements you have and this type of highly threatened environment to make those —to measure

those successes is the type of person we were looking for and is precisely the reason we were looking for them. It is all about metrics.

Mr. ETHERIDGE. Thank you, Mr. Chairman.

Mr. THORNBERRY. Thank the gentleman.

The gentleman from Georgia.

Mr. LINDER. Thank you, Mr. Chairman. I only have a couple of questions on this idea of sharing intelligence and information.

I think we are beyond the stage where our intelligence agencies are not sharing with each other. Is that fair to say?

Mr. LISCOUSKI. Yes, if I heard you say, we are beyond the point where we are not sharing.

Mr. LINDER. Yeah.

Mr. LISCOUSKI. Implying we really are sharing the information. Yes, sir, you are correct.

Mr. LINDER. How good are we at analyzing what we are getting?

Mr. LISCOUSKI. At what level, at the physical level or the traditional threat level or at the cyber level, sir?

Mr. LINDER. The threat level.

Mr. LISCOUSKI. At the traditional threats level, I think we are very good at analyzing it.

This is an extremely difficult problem, and I can speak to it some, but I really defer to my colleague, Bill Parrish, the Assistant Secretary for Information Analysis, in his domain. But I have operated in this space for quite a long time, and our capabilities for analyzing information have only increased over the years. I mean, we have gotten very good as a whole, as the Intelligence Community, to analyze information.

It is an extremely complex problem because you never have the perfect information. You can never do the perfect analysis. You can only do it in hindsight and retrospect. It is an extremely difficult problem to solve. But I think the capability is the people we have attracted into the Intelligence Community, particularly in DHS, are really some of the finest minds out there to be able to understand these complex problems.

Mr. LINDER. And lastly, how cautious or how careful are you in sharing this with first responders? There was a time when they were being overburdened with unanalyzed intelligence right after September 11 to the point they just set it all aside, and it had no value whatsoever. I think you have to be careful what you give to them, that it has to have some specificity, some analysis, and that it is right down their alley.

Mr. LISCOUSKI. Yes, sir. In fact, our focus is not on first responders, and I don't mean this in any other way than calling them first preventors.

When we are sharing intelligence information, it is really intended to prevent the act from occurring, and we will err on the side of sharing probably too much sometimes. Of course, not in the sense of sharing classified information inappropriately. But working with TTIC, IA, the FBI, we have been very aggressive in assuring we can quickly declassify information to share out to the field, to our consumer base, as quickly and as effectively as we can.

That is a challenge we are always going face. Sources and methods, as you well know, are one of those things—that is something

that has to be guarded very carefully. But I believe—and I have seen it in practice—that we will err on the side of maybe sharing too much information sometimes, because the frustration you can create by sharing general information without specifics, and particularly with specific activities to follow, sometimes can create a frustration. But, nonetheless, I think as we all mature in this process, particularly as our end users understand the context during this threat environment, they themselves will raise up their capabilities as well.

Mr. LINDER. Thank you.

Mr. LISCOUSKI. Thank you, sir.

Mr. THORNBERRY. Thank the gentleman.

Gentlelady from the Virgin Islands.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman.

I want to welcome the Assistant Secretary and thank the chairman and ranking member for holding this hearing, given the recent attacks, like the Blaster worm, and the concerns that even a worse attack could occur within several hours or days and the fact that so much of our physical infrastructure is dependent—is so cyber dependent.

It is an important hearing, and I want to applaud you, Mr. Assistant Secretary, for your focus on ensuring that cybersecurity and physical infrastructure security are linked in your operation, as it is important as they are linked in reality.

I have a couple of questions. One of the—we have been concerned about the slowness of the Department in getting started and being able to plan and address many issues; and one of the obstacles to that has been the fact that we were bringing together 22 agencies and trying to blend them into a smooth operational unit. The NCSD brings together about five different parts of five different agencies—FBI, Commerce, Defense—as well as a center. Are you pretty comfortable that some of the obstacles of bringing different agencies with different cultures together has been addressed and that you are able to move forward smoothly now?

Mr. LISCOUSKI. Yes, ma'am. I will tell you why that is a great question.

I am satisfied because—I mean, that has been tremendously challenging. I mean, bringing these organizations together under one roof has been something that I don't think any person who even architected this in the planning stages understood the complexity of it.

I can speak for my own area within IAIP. As you pointed out, we brought five different organizations into the NCSD and IAIP. I just remind everyone respectfully that we have been in business for 6 months, and the challenge we face in trying to overcome some of those organizations has been pretty daunting; I've got to be honest with you. I mean, when I came in from the private sector to do this, it set me back a little bit when I thought about, How are we going to do this and how are we going to do this in the context that we have a real threat we are facing every single day?

If you recall, when we did this, we were at war; and we had to organize ourselves around work to respond to very real threats in addition to bringing people on, creating organization. It was pretty challenging.

The leadership at DHS, the senior leadership of DHS, provided the right latitude in order to make mistakes. And that is what we are going to be doing. I mean, clearly, as we start out with this organization what it looks like today, in 2003, will probably be a lot different in 2005, 2010. And hopefully if we are succeeding we are going to continue the path of evolution that will eventually evolve DHS into the robust organization it really does need to be.

But we are on that path. It is a long road, but it has been good. I mean, I can tell you in my private-sector experience the thing that has been kind of very helpful to me is knowing that we are going to make mistakes. But we don't have the luxury of not making them. In fact, when we tell people when they come on board—and I have said this before, I think, before the committee—that we have got sort of one thinking. It is a think big, act small scale, fast.

We know we are going to make mistakes. We know we have to learn and we are going to evolve. It has been gratifying when you look at it; and we were, on the way over here, reminding ourselves it has only been 3 months for the division and it is been 6 months for the DHS. In dog years it seems like it has been a lifetime.

I can tell you that right now, it has been pretty challenging, but we are making some very tremendous progress.

Mrs. CHRISTENSEN. The other concern that I have is, the officials who have left the positions over the few months; and is, related to this, the difficulty in bringing the Department together? Have you identified what the fault is, what were the problems that would cause these officials to leave?

As you were looking for a Director of the NCSD several candidates had indicated they weren't interested because it was too far down the chain; they didn't have a direct link to the Secretary.

Have you identified what it is that needed to be fixed? Because the continuity of leadership is critical.

Mr. LISCOUSKI. Yeah. I would suggest that I am not so sure it needed to be fixed as much as we just had to find the right person that understood this is about execution.

The challenge we had was taking a strategy, a highly articulate and well-developed National Strategy to Secure Cyberspace, and then putting implementation plans for that strategy for execution. Two different types of people are required for that job. And it is really difficult to be a strategist at one level and an implementer at another level; and we needed an implementer, and we needed a start-up person that could take something where, to be quite candid with you, is now somewhat of a chaotic environment, when you start things up and just make some very short-term, measurable progress. And that is the type of person we were looking for.

So I don't think there was a problem as much as there was finding the right talent to fit that. And it is a challenge, and it is a very risky challenge, because, you know, Mr. Yoran is coming in to us with very definable goals. We have got high expectations. It is very visible. And the risk to him—is you know, at a personal level in terms of potentially not succeeding, as well as to the Department is great.

So it is—when you are out there publicly like that, not many people really want to take that challenge on.

Mrs. CHRISTENSEN. Okay. One last question in this round. Reading some of the articles in our background material—and it is also my feeling that the Federal Government should lead by example in cybersecurity—where are we in identifying the risks and vulnerabilities of the government's cyber assets? Are we leading by example?

Mr. LISCOUSKI. Leading by example; I think we are probably on a path to leading by example. I suspect there is always a lot of room for improvement. We do have efforts underway to do that. I think FISMA—the law has provided us tremendous guidance and leadership or a framework from which we can operate to ensure we are doing the rights things. So from that perspective I think, frankly, FISMA is a wonderful example to look at as a guide across the board. So I suggest the government is leading by example on that, in that realm.

In our purchasing requirements, our ability to justify our programs based upon good security practice, are things that I think are very rational approaches to take as it relates to cybersecurity. So I would argue, yes, I would think that the government is leading by example.

We can be doing better. Cataloging our infrastructures, understanding the interdependencies, those are things we are trying to do across the board, and we have got programs in place to do that. I think we will be getting better as we move along.

Mrs. CHRISTENSEN. Thank you.

Mr. THORNBERRY. I thank the gentlelady.

The gentleman from Kentucky, Mr. Lucas.

Mr. LUCAS. Thank you, Mr. Chairman.

Mr. Secretary, in June you had detailed the plans for Consolidated Cybersecurity Tracking Analysis and Response Center that would detect and respond to Internet incidents, track potential threats and vulnerabilities, and coordinate cybersecurity and incident response for the Federal, State, local governments, private sector, and international partners.

What has been the status of the center?

Mr. LISCOUSKI. Sir, the CSTARC, the Cybersecurity Tracking Analysis Center, has evolved into the US–CERT. That was a preliminary step for us to be able to organize ourselves around this effort, consolidate the watch centers and the efforts we had within the other organizations that came to us when DHS was created—those organizations being the NIPC, the CIAO, elements of the NCS, the FedCIRC—into one organization. And that CSTARC represented the first iteration of what we knew was going to become the US–CERT. With the CSTARC we were able to very capably manage a number of significant incidents, the SoBig, the Blaster virus, the Cisco vulnerability. And then that, as I indicated, provided the framework for us to be able to build on that to create the CERT, the US–CERT.

Mr. LUCAS. This is a hypothetical. In the event that we had a terrorist incident today, a cyberterrorist event, could you just explain to me what process we would use today to notify all these different interested agencies?

Mr. LISCOUSKI. Yes, sir. In the hypothetical example, suppose we were notified in the private sector that they first identified a par-

ticular exploit, and that exploit resulted in our analysis to determine that that might be something that would be used or may be the focus of a terrorist attack. The combination of resources we have across the Federal Government currently, if it comes to DHS first, our analysis capabilities, leveraging on the US–CERT to understand those exploits is our first stopping point. The US–CERT then quickly engages with other components of the Federal Government, the JTF, CNO, for cooperation and additional analysis. We would reach out to the private sector to do additional analysis. And as quickly as we get our analysis completed to determine what the vulnerability or the threat might be, then DHS has got the advisory capability of putting warnings out very quickly to the entire community vis-a-vis its alert system as well as the ISACs to ensure that we have got thorough coverage.

And, again, it is a work in progress. I am not suggesting it works the way it should work all the time or it is as thorough as it should be. Over time, our goal is to ensure that we increase that coverage.

Mr. LUCAS. I understand you said you were staffing up. You have about 65 now, and you are hoping to have 100-plus.

Mr. LISCOUSKI. Yes, sir.

Mr. LUCAS. So, do I take it from that that you feel that you have the financial resources you need to carry out your mission? Or, if you had additional financial resources, how would you utilize them?

Mr. LISCOUSKI. You could always use money, but I am not so sure if adding more money at any point in time is necessarily the quickest solution. The biggest thing you have got to do is build the right framework in the right organization in which to put people in in the partnerships.

I think we are adequately funded right now. I think we have got the right path to go on. We can come back and address that downstream in fiscal year 2005.

Mr. LUCAS. Those are my questions.

Mr. THORNBERRY. I thank the gentleman. The Chair recognizes the Vice Chairman of the subcommittee, Mr. Sessions.

Mr. SESSIONS. I thank the Chairman and appreciate him holding this hearing today, along with the Ranking Member.

Mr. Liscouski, welcome. We are delighted to have you here today. And I would say to you, and I think you have heard this from members, we appreciate your private sector experience and the things which you learned there and the focus that that brings to you and the DHS; I think that the Federal Government will be better off because of those lessons that you have learned.

I would like to focus my questions today; I just heard you use the word "framework." Some people could also say the word "business plan" might fit in the middle of that, framework business plan.

On page 2 of your testimony, there are six different pieces that are called status of integrating organizations and functions below into DHS. And it talks about the elements of the National Infrastructure protection center—formerly housed in the Federal Bureau of Investigation—DOD, FEMA, Department of Commerce, Energy, and General Services, GSA, into functions that you are evidently going to be responsible for.

I am interested in your discussion with us about the word "framework," about how you are going to bring these functions in to make sure—I guess the best word is to say, "to measure twice and saw once" for the efficiency and the effectiveness so that we are not recreating something 7 or 8 or 10 months down the line because of your need just to rush into service.

Would you mind discussing those things, those activities of those six different pieces.

Mr. LISCOUSKI. Sure. And this is broader than cyber, sir. This really relates to the entire Infrastructure Protection Office. And I would be happy to address that because I think I have got to talk about that, and then the framework for the other divisions fall out of that.

Generally speaking—and I will go back to the very beginning when I came to DHS back in March—as I indicated, it was obviously brand new. We had been involved— when I got there it was about 3 weeks old. So—and we were in the middle of a war and we were staffing up to respond to the threats we had.

It was immediately apparent that the work that we were engaged in could not change substantively, because the same elements that came to us from the Energy assurance office, from the NIPC, from the CIAO, from the NCS, those elements were the very elements that were responding to the threats of the present day. So we had to be very careful as we were building this framework and identifying what our bigger mission requirements were that we didn't break anything. So that was job one, and make sure that we responded to those threats.

So in our current-day thinking, what we did was basically establish a capability that would operate at one level, which was just putting one foot in front of the other to make sure we were not stepping on a land mine, so to speak, and we were executing against the goals that we had against that particular threat.

Now, by the same token, we had to also think in a bigger picture to understand what did the organization need to look like over the 6, 12, or 18 months? So we began to develop an organization based upon the work that we were in. And that was the first question: What business were we in? You know, were we out there doing vulnerability assessments; were we just out there thinking great thoughts about protection strategies we should be doing? How do we create a capability that could address critical infrastructure vulnerabilities across 13 critical infrastructures, 5 key assets, the cyber environment, in a way that we could put coherence around this?

So we were able to organize ourselves at the first level to understand what the organization needed to look like. It started off with a very basic line of block chart with two organizations in it. We added a third. We kind of mixed it up. I mean, we really learned as we were going.

To your point, we wanted to ensure that we acted quickly to identify the immediate needs but as we built an organization for the longer term. We are exactly in that process right now. I now have four divisions in my organization, because we have identified the need to build it out but yet stay integrated; not specialize too

much, but orient ourselves according to sort of our business approach.

And I can get into some more detail if you would like. But effectively what we started doing was a supply chain analysis. We looked at our client base and we looked at the private sector, the Federal sector, State and local governments, the territories. We looked at all those client bases and determined what was it we were delivering, what was it they needed, and how do we deliver it and what were the inputs into that delivery system, into the production system. And that is precisely what we are doing.

So we are still going through that process. I suggest it is going to take a few more months before we really figure out the exact processes we need in terms of an organization. And then, as I said earlier, this organization is probably going to evolve as we learn more about our businesses as we go along. It will be a continuous work in process, I can promise you that.

Mr. SESSIONS. You know, I think some of my comments—and I don't presume to know the things which are important necessarily to each one of these elements, not being aware of all the databases; but it is my hope that you would be able to develop in some efficient factor a database with firewalls with the elements that you need to avoid six database administrators, six of everything to accomplish these things.

And that kind of goes back to the framework that the house—the sandbox you are going to build. And it is my hope that really your private sector vision would allow you and the assistant secretary that luxury to please make sure when you build that, whatever it is, that you do it within that framework. And I guess my last comment is very plain. And that is, we heard testimony last week where the people who were in charge didn't communicate what they were in charge of, didn't tell anybody what they needed to be doing, and there was a failure from top to bottom, command-and-control structure. And it is my hope that you really do follow up with those things of integrating yourself with business leaders and commercial leaders in this country to make sure they know not only what you stand for but the lessons learned; because I think that the key to this is avoiding or being prepared to avoid a strike that would cripple this great Nation.

Thank you for your service. And we appreciate your being here today.

Mr. LISCOUSKI. Thank you, sir.

Mr. THORNBERRY. The gentlelady from Texas.

Ms. JACKSON-LEE. I thank the Chairman and Ranking Member again for holding a very vital and important hearing. And Mr. Liscouski, thank you for your willingness to accept what I think is a larger-than-life challenge. It is something that I hear when we travel. We had some hearings, field hearings in Los Angeles and Long Beach, looking at the ports; and cybersecurity technology permeates every aspect of the needs of homeland security. And I am hoping that you are getting that sense by the position. And I am going to take a line of very rapid-fire questions and a series of them, and then if you could try to respond.

One of the questions already asked about being able to coordinate, if there was a cybersecurity or cyber attack, coordinate with

respect to our own Federal agencies. My pointed question is: Do you feel confident that you have the authority, in essence the power, to be able to command forces that deal with cyber issues in a time of a cyber attack? And I really want you to be pointed on the question of authority, because that is our responsibility. How can we assist you to do that? Because it certainly is telling that we have had a trail of back—the back of people's backs—and that is departures—respecting their reasons for doing so, but that is what has occurred. So it is a great concern to me that you be vested with the authority to do the job.

One of the things that the Federal Government has as its assets—it has many assets, but it has several that relate to homeland security and terrorist attacks. Certainly it is a role model in action. So goes the Federal Government, so goes the rest of the community in terms of looking to how we respond.

They watched us on 9/11, and I think we are quite grateful that we were able to muster our senses about us and maintain the continuity of government. The Pentagon was excellent in the face of tragedy, and we all tried to support them and go forward. But that was looked upon.

We also have the bully pulpit as to how we can encourage communities to pull up their boot straps and get going on some important issues. So I want to know specifically about the authority.

Let me also say that—have we made and do you have under your belt the enunciated vulnerabilities of the Federal Government; specifically know where the cracks in our armor is? We wanted to come and either have you delineate those—and you might give them to me generally—but if we wanted to have a closed-door session where you said, really pointed out some of the large gaping holes, could you today, September the 16, 2003, list those for us? Very vital. Because as I said, if the government collapsed in the midst of a tragedy, we are certainly sending a bad signal out to those who are struggling to overcome whatever the problem is.

Rapid fire, I continue. Have you found any connection to cyber problems with respect to the massive blackout? Are you engaged in a collaborative effort in that investigation?

What would be your response to the fact that we are raising brighter and more inquisitive teenagers? I cite the 17-year-old in the western State who was part of the virus epidemic. Of course, everybody is talking about what a great young man he is; he didn't mean it. But they are everywhere.

How are we dealing with the potential of this bright emerging army of detractors? And do we do an outreach campaign?

Do we work with schools? How can Homeland Security be of help to you on that? Do we have a doctor in the House? Are we able to have our researchers and doctors look at—and when I say "doctors," I put quotes around it—look at the next virus on the scene? Why are we only reacting? Our Nation is going to look to us to be preventative medicine, so why are we in the same boat as my BlackBerry ran away with itself a couple of weeks ago with it is coming, it is coming, it is coming? No solution, but it is coming. I think we need to be in the business of preventative medicine. Who are we retaining? What kind of resources do you need to be able to be the predictor of what is to come?

And, finally, we did something in a bipartisan manner last week that I am very proud of, and that is the Fair Credit Act, I believe. But a big piece of that was the protection against identity theft. But we can't do it alone with an authorization bill under financial services.

I believe that identity threat is a threat to the homeland security because why? Terrorists can steal your identity and walk around and be as unpredictable as possible. What are we doing with respect to identity theft which comes a lot through the computer? And I thank you for responding to these rapid-fire questions.

Mr. LISCOUSKI. Thank you, ma'am. If I took them down right, I will be able to respond to them intelligently, hopefully. First, I have to be able to read my own handwriting.

With respect to coordination, and specifically with respect to the question of authority, I want to clarify one point. DHS has got authority, protection authority. By statute, the Homeland Security Act has set DHS up to be the promulgator of protection strategies. From an investigative standpoint, we partner up with the FBI, with the Secret Service, which is clearly part of DHS. But the FBI has got the lead in many of these cases to— and this is where we probably need to get in a little bit of a closed-door session, I think. But at the top level, the authorities that we have, clearly I would say we have adequate authorities to ensure that we have protection on our cyberspace. And I say that in a thinking mode primarily because we are just in the execution phase of our strategy. And I think time will tell whether we have the appropriate—whether we are impeded from executing fully the strategy that we need, as has been articulated in the strategy and as we have identified it. But I would say right now, yes, DHS has been provided the full authority that we need, there are some excellent programs we have in place and that we have in plan, that are not appropriate for this session, that I think really can articulate what those authorities are and how we are meeting those things.

As it relates to responding to an attack and what that might imply for other activities the U.S. Government would be engaged in to prevent or actually to intercede or interdict a cyber attack, those are resources which are not just owned by DHS but other components of the Federal Government. So again, that might be a more appropriate discussion for a closed session, if you can indulge me on that.

On the second point: Have we made a full analysis of our vulnerabilities? Again, I can tell you it is a work in progress. I don't think we will ever know. I mean, the context of a full analysis of our vulnerabilities implies that we can get our arms around these things. And in the dynamic and ever-changing environment in the technology world, new vulnerabilities are always going to be coming out. And the challenge we have is not just articulating or clearly identifying and articulating those vulnerabilities in a steady state. But there is no such thing as a steady state in the technology world you identify with the vulnerability of a nuclear power plant, because typically that technology doesn't change. The threats to the nuclear power plant are not necessarily static, but there are only so many ways you can attack it. In the cyber world, it is very dynamic. So that will be a continuous work in progress.

We have our hands on what I think is a good fund of information that articulates what our vulnerabilities are in the government, and clearly we are working hard on that. Again, that might be more appropriate discussion for a closed session.

With respect to the blackout, again I have to apologize. In fact, I guess I will be coming back tomorrow at a different committee hearing to discuss the blackout. I am not at liberty to say what we have found in terms of root cause and what the respective relationships are in the cyber components. That report will be coming out. I believe there will be an interim report here in October, and that will be published by DOE and the task force. I will have to indulge you on that question as well.

An interesting point you brought up about the teenagers and those who are propagating viruses and the relative ease they have with which they can do that is a serious concern. You have got a number of different types of viruses that can be created out there. One is just basic tool sets that people pick up off the Internet. They get bored with—they decide they want to cobble them together, and they create a virus, and that can happen fairly quickly. There is a different one, a different set, different mind-set of people who decide they want to do this, and then just quietly make them available to those in the quote -unquote teenage realm here that you described, that they are not even smart enough to maybe make their own viruses; they might evolve them a little bit, but they are not the original architects, and then all of a sudden these viruses find their way into the public domain. I think our authorities, I think the law enforcement community needs to aggressively pursue these people.

I think this is similar to a discussion I had with some advocates in the private sector who operate in the security space, that they really want to see the government, the law enforcement community, go after folks who provide the basic tool sets, the basic know-how to anybody on how to propagate a virus. This is similar to becoming a conspirator in a crime.

Somebody mentioned an excellent example. If you are the driver of a getaway car in a bank robbery and a passenger, your codefendant, decides to shoot somebody and kills them, you are equally as guilty as the shooter, just being the driver. We should probably take the same attitude toward people who propagate viruses. This is serious. And when you talk about billions of dollars' worth of damage and losses to the private sector and the government, these are no light matters. We need to take this seriously.

The doctor in the house, the capability that we have in the research community of developing the right talent, I think DHS partnered up with others in the community, DOD in particular, creating centers of excellence, providing scholarship programs for cyber—you know, in the information security world. It is a tremendous step forward. Do we need more people? We absolutely need more people. And I think we are making the right steps to address those needs.

And your final question: The Fair Credit Act and what are we doing to protect against that? Again, I think there are good efforts going on in that space. I think the FTC, and I know Orson Swindle in particular, has been very aggressive in putting the word out

about what consumers need to do to protect themselves. The Secret Service operates in the identity theft space.

I agree with you, it is a very, very important issue. It gets back to the issue about privacy and how you protect privacy, and that is a central component of information security. You cannot have privacy without good information security.

So,I appreciate your questions.

Mr. THORNBERRY. The gentleman from Rhode Island.

Mr. LANGEVIN. Thank you, Mr. Chairman. And I want to join with my colleagues in thanking the Chairman and the Ranking Member for organizing this hearing. And, Mr. Secretary, thank you for being here as well.

If I could, you had said that home and broadband users are one of the groups you would like to focus on outreach and education. And certainly, without a doubt, they are one of the greatest neglected weaknesses in our national plan to secure cyberspace. Can you give us a better sense of how DHS is planning to address this? And would it be appropriate to work with, for example, the Federal Trade Commission, which, as you may know, is also mounting its own "stay safe on-line campaign"? And do you feel that a large-scale public awareness campaign needs to be launched? And, in particular, and following up with one of the points my colleague from Texas made in terms of reaching out to young people, and maybe through demonstration programs, how we can involve young people in these awareness campaigns and kind of harness their energy and natural ability to work with computers? I think that would be a good place to start.

And one other point I would like to address, and this may have to be addressed in closed session, but I think it is an important point of focus. And that is in your vulnerability assessment on our national assets and other areas. We have seen a trend in recent years worldwide among terrorist attacks, that terrorists focus on high-casualty, high-shock value events. And I am curious and I think we all need to be attentive to what those areas are in the world of cybersecurity that fall into that realm. There may be only a few areas that would compare to the use of a WMD in the cyber world, but those are the things that I think we need to have high priority and focus on.

And I would like to at some point, even if we can't do it here in open session, to follow up on that. And I think that would be important. Thank you.

Mr. LISCOUSKI. Thank you. I am just trying to read my own handwriting—your first question.

Mr. LANGEVIN. It was on your comment earlier that home and broadband users—.

Mr. LISCOUSKI. Do we need a large-scale—exactly. With respect to the broadband, one of the things we are working with the National Cybersecurity Alliance. Among those representatives on the Alliance are ISPs, AOL, and others. And they are taking an individual responsibility to educate home users to the challenges and security challenges they face in broadband connections. I would like to see that expanded. I think there is no question that the broadband community, you know, the commercial space there needs to be really—from my point of view, I need to use the bully

pulpit to get them to understand their responsibility that, as they sell broadband connections, they have got to provide better awareness notices to their users about the potential damage that can be done.

Because it doesn't just affect the individual. As you are well aware, the individual user—these viruses propagate very quickly, and consequently can spread across—using zombies or using personal computers that are accessible via broadband connections and then propagate these attacks. So there is a real, I would suggest almost fiduciary responsibility on their behalf. But that might be a little bit too aggressive. But at the end of the day, we need to put that awareness and that responsibility with the ISPs and the broadband connections, cable companies, et cetera. So I do certainly agree with that.

The educational efforts, the outreach efforts, from our point of view are geared toward educating the consumer. Your point about young people and education, I liken that to, you know, the DARE program, the Drug Abuse Resistance Education program that has been around for—must be 20 years now.

Educating kids—and this is clearly a different perspective. We are moving from self-esteem to responsibility and how do you act. But I agree. I mean, it scares me to death to know that young kids are on these Internet connections not knowing about the dangers that they face through going to chat rooms and the vulnerabilities that they have there. I mean, just the vulnerabilities of kids being on the Internet is something that scares me. And that is something that we can address through good education programs in the schools.

DHS is going to be working hard to figure out how we do that and reaching out to the schools to provide good awareness and good education programs. Fortunately, the NIPC did this previously. We have inherited those programs so we have got a basis for doing that, and I think they have been successful. They have got poster programs. But we need to expand that. It is a high priority for me personally.

The vulnerability assessments, the trend in recent years that you have articulated. Clearly, you know, I can get into depth in this in a closed session, but at a top level we do worry about the combination of a physical and cyber attack. You know, a cyber attack preceding a physical attack, taking out a 9/11 system and then combining that with a physical attack. You know, it is a scare. Is it doable? I would say at this point anything is doable. And it is something we worry about a lot. And we are working down—I can tell you one thing we are working very aggressively on is—and the categories of all the critical infrastructure we really worry about—we look at what the nexus would be with a cyber attack to see how that might be enhanced or what that sequence might look like.

Mr. LANGEVIN. Thank you.

Mr. THORNBERRY. I thank the gentleman.

Mr. Liscouski, I would like to—first let me ask this. Before you took office, the administration put forward this document, which is the National Strategy to Secure Cyberspace, dated February 2003. So far, have you discovered a major gap or something that—where you think the emphasis was not placed, the proper emphasis was

not placed in this document? Or is this something that you can still go by today?

Mr. LISCOUSKI. No, sir. It is still a very valid document. A lot of good thinking went into that, and I think the private sector's input into that became particularly valuable to me as we thought about how we needed to create our national cybersecurity division.

Mr. THORNBERRY. Well, I would like to just briefly—and this will entail a little bit of repetition from what you have already talked about—but I would like to go through those five priorities and ask you to kind of give us a snapshot of where we are with each of them.

For example, the first priority listed in that document was a National Cyberspace Security Response System. And they talked about a public/private architecture where you would analyze attacks and warn and manage incidents and then respond. It sounds to me like that is essentially what US–CERT is going to be doing. Is that the primary way that we are going to implement that priority?

Mr. LISCOUSKI. Yes, sir. It is the foundation for it. The US–CERT is clearly the linchpin for that effort.

Mr. THORNBERRY. And then what more needs to be done?

Mr. LISCOUSKI. Well, we need to—clearly, building relationships at the private sector. I think the US–CERT is an excellent start at that foundation. And we have engaged in discussions with the private sector, the Nortons and the McAfees of the world, to determine how we can integrate their contributions to this effort. I think there is a lot of good work that can be done there.

The private sector is doing a tremendous amount of good information collection and analysis on viruses and vulnerabilities that we would like to be able to integrate more robustly. And then extending the information out—as we spoke earlier, the National Response System is not just national but it is international as well. So we have a lot of work to do there as well, sir.

Mr. THORNBERRY. The second priority is a National Cyberspace Security Threat and Vulnerability reduction program, where the National Strategy talks about reducing the threat, identifying vulnerabilities, and then trying to develop systems with fewer vulnerabilities. Give me a snapshot of our efforts to implement priority No. 2.

Mr. LISCOUSKI. Again, and you know, the dominant theme here is private sector. And we have to again work with the major manufacturers and the smaller manufacturers of both hardware and software technologies to ensure that when they produce technology, it is according to guidelines and expectations that they have fewer and fewer security vulnerabilities. And if we can—and to be candid with you, companies are stepping up to that challenge. You know, pointing out to Microsoft and the things that they have done, they have taken this responsibility. I know they have been subject to a lot of criticism, but at the end of the day they are—their chief security officer is responsible for overseeing many of the programs that they have. They have taken very good steps here.

It is a good example of what we need to be doing with the private sector. Those who produce it have to understand that they have the responsibility of producing good technology the first time around.

Security defaults should not be off. I mean, this is the classic thinking of just basic things that need to be done. They are making good inroads there.

The other point is to continually look at the infrastructures, you know,the vulnerabilities that we create by implementing technologies. I mean, this is a bigger discussion, to be quite candid with you, but we are doing a lot of analysis as converging technologies come in. I mean, we look at the convergence between the IP world and the telecom world and the vulnerabilities that are inherent there, because of—and forgive me for going too deep into this. But just as an interesting example, one of the advances of technologies, because they become more efficient, they themselves bring about vulnerabilities because now one device can do the work of 10. Where you had redundancy before, now you are down to a critical path of one device as being a key vulnerability. So we are constantly looking at those things as well.

Mr. THORNBERRY. Talking about the private sector, at this point, do you have an opinion about whether market forces are going to be enough to elicit the kind of response from hardware and software vendors that the country must have?

Mr. LISCOUSKI. I am optimistic that the market forces will be sufficient. But I am prepared to say that if they are not, we need to quickly adapt our thinking.

Mr. THORNBERRY. And as part of that reduction of vulnerability, is the Department looking at physical infrastructure related to cybersecurity as part of our vulnerabilities and part of what we need to assess?

Mr. LISCOUSKI. Yes, sir. And, unfortunately, this has been going on prior to even the establishment or the articulation of a national strategy. The NCS, the National Communication System, which was previously a DOD component, did a significant amount of work on vulnerability analysis of the telecom industry and then the IP backbones. So we have got a significant amount of data here that already allows us to be able to identify these vulnerabilities, and we are continuing to expand that.

Mr. THORNBERRY. It seems to me greater work is going to be needed in that area, and we can discuss that at another time.

Mr. LISCOUSKI. Yes, sir.

Mr. THORNBERRY. Let me briefly go through. The third priority was a Cybersecurity Awareness and Training Program; a number of questions have dealt with that so far. Is that going to be the focus of your summit in the fall?

Mr. LISCOUSKI. That is a key component of it—for us, understanding how we can better reach the community. And our summit is going to include not just those in the technology industry, but across industries, so we have a broad approach to understanding the problems. So, yes, sir.

Mr. THORNBERRY. The fourth priority was securing government's own cyberspace. You have been asked about that before. But I am unclear, frankly, as to how much authority or influence you have in bringing the rest of the Federal Government along. My understanding is that that has been primarily OMB's responsibility. And just about every witness we have had before this subcommittee says that the government is nowhere near where they should be,

and that if the government would lead, it is such a big consumer and has such market power, that it brings the rest of the country along with it. But what is your role exactly in bringing the rest of the government along?

Mr. LISCOUSKI. Our role is really to support the OMB. OMB does have the initial lead to ensure that, through FISMA and through the regulations that they provide and the oversight, that the government is responding to their responsibilities to provide security. DHS's role in this is really to coordinate the incident response and warning through the FedCIRC through the Federal Government, and I think that could be expanded to understanding more about the vulnerabilities.

As I indicated earlier, we do have the patch for remediation responsibility through the PATC to ensure that the right tools are available to the government. So we have a responsibility there, sir.

Mr. THORNBERRY. The final priority was national security and international security cooperation. I don't know—you have alluded to those things briefly before in your testimony. I suppose that is an area where there are an ongoing efforts and will have to continue to be ongoing. Let me ask you to do this. Rate where you believe international cooperation is on cybersecurity at this point.

Mr. LISCOUSKI. I had said in the beginning stages, it is tough to put a numerical code on it. I would say we are really in the beginning stages of understanding—well, we clearly know what we need to do, but we are just in the very beginning stages of really making some progress and establishing the relationships that are so necessary for us. There is a lot of opportunity there for us. It is a big world. I mean, there is a lot. And as you pointed out earlier, this technology is ubiquitous. It is not necessarily discriminating by economic income in terms of gross national product. I mean, you can get cheap technology out there and create these vulnerabilities. So we have a lot of work ahead of us to do, and I think we are positioned to do it.

Mr. THORNBERRY. Thank you.

The Chair recognizes the distinguished gentleman from Florida, Mr. Meek.

Mr. MEEK. Thank you, Mr. Chairman. Thank you, Mr. Secretary, for being here.

Speaking of the private sector, and I guess when we speak of the private sector we are just not talking about domestic private sector, because the cybersecurity is a huge issue. Recently, as you know, with the New York blackout you had thousands of New Yorkers in subways and you had folks in Detroit and auto plants that were shut down, and it halted after-hours trading as it relates to Wall Street. A lot of things took place. What exercise did the Department go through to find out was it or was it not a cyber attack? That is one.

Two, what happened in the private sector as it relates to that, especially in our energy industry and those that handle their cyber needs? What took place as it relates to checking, making sure that we weren't under a cyber terrorist attack?

Mr. LISCOUSKI. Okay. If you can indulge me, I have to speak in general terms.

Mr. MEEK. Sure.

Mr. LISCOUSKI. We are in the process of investigating that component. I chair the Security Working Group for the Electricity Task Force. So, in that capacity, I have got to be careful what I can say and what I can't say. We are going to have a hearing tomorrow on this and we are going to be publishing reports downstream, so I want to be a little bit circumspect. But what I can do is discuss what we did as DHS during the blackout, and I might add some clarity about how this process works a little bit, because I think it is clearly relevant and it is not going to be disclosing anything that can't be disclosed.

I am quite proud—I mean, DHS should be very proud of how we came together to respond to the blackout along with the rest of the Federal Government. But DHS in particular was sort of the point in contact in understanding what was going on in the industry. We immediately reached out, upon learning what was going on, to the industry to determine what was their perspective. I mean, it is the unique thing that DHS has the ability to reach, through the ISAACS, to the private sector, in this case the NERC, to determine what is going on and what is the situational awareness component that we need to respond to. Do we have a terrorist event? Because precisely how we are positioned to respond is, you look at an event like that, then you immediately go to the next step of saying what can occur next? Is this a terrorist event? And even if it is not, A, could it be exploited? Or, B, if it is a terrorist event, what is the next step? And we immediately have the capability to do that.

So DHS was able to come together very quickly across its directorates, ask those questions, gain situational awareness, and provide direct advice to the Secretary and subsequently to the President about where we were. And then working with the FBI, the combination between DHS and FBI, we were able to quickly conclude from an initial perspective that there was no terrorist nexus there.

Mr. MEEK. So were you pleased with the checking process as it relates to is it terrorism or is it not terrorism amongst many departments and even the private sector?

Mr. LISCOUSKI. Yes, sir.

Mr. MEEK. So this report is going to be based upon trying to better what is good already? Or what areas will you be looking at?

Mr. LISCOUSKI. Well, the report is not examining how DHS or the Federal community acted. We are really looking at the root cause of the blackout.

Mr. MEEK. And its potential for taking place again?

Mr. LISCOUSKI. Correct. That is correct.

Mr. MEEK. As you know, with the World Trade Center, there were many attempts and sometimes folks get great ideas. Will there be any discussion on how to not only share with New Yorkers but Americans when an attack like that takes place—as you know, the power was out, there was no cable television for folks to look at, there was really no communications whatsoever. Will that be something that DHS will be looking at, to see how can we contact—I mean, everyone you hear, oh, New Yorkers, they did their thing, things went very smoothly, people knew where to go. But there was a lot of street hollering on the corner on how do you get out of Manhattan.

Does the Department's looking into reaching out and to individuals need to be through two-way pagers, through the telephone, through things that were working?

Mr. LISCOUSKI. Yes, sir. In fact, that is really within the domain of Emergency Preparedness and Response Directorate under Secretary Mike Brown. They are looking, they are doing a deep look about that type of communication requirement, first responders, et cetera. I would really defer to them.

Mr. MEEK. Okay. One last question, Mr. Secretary, or I guess a concern of mine. I just want to make sure that cyber partners that we do have that are working with us against this effort in terrorism, that they are working as hard as possible and together. I look at what—your job is almost similar to almost the Intelligence Community. It is kind of hard to share information. You have competition, you have private sector needs and technology needs and things that they want to keep to themselves. But if is not put on the table on behalf of security as it relates to the cyber world here in the United States, we may very well have problems. And when we have a problem, that means that things will be legislated and decisions will be made in haste that individuals may not like. And I think it is important that we encourage them to work.

I wish you well on your report. I am looking forward to seeing and hearing more about it.

Mr. LISCOUSKI. Thank you.

Mr. MEEK. Thank you, Mr. Chairman.

Mr. THORNBERRY. I thank the gentleman, and want to mention, again, that this subcommittee as well as the Border Subcommittee will hold our second hearing tomorrow on this interdependency of infrastructures. And Mr. Liscouski will be one of the witnesses, as well as others from the Department, because I agree with the gentleman from Florida; these are critical issues and we need to learn the lessons when it happens the first time so that we are not put at a disadvantage.

The Chair would recognize the Ranking Member.

Ms. LOFGREN. Thank you, Mr. Chairman. A lot of the questions I thought I would ask have already been asked, so I really just have two issues that I want to raise. One has to do with the ISACs. You mentioned them in your testimony. And the feedback I have received from the private sector is that some of them are performing a lot better than others. And that, in particular, telecom actually seems to be working pretty well, IT; but, in the other sectors, that they are basically not functioning. And—and I don't know if this is true or not, but this is what some of the private sector people have said—and the problem may be a lack of funding support. At least that is what some of the private sector people identified.

Do you think that that assessment about some of these ISACs is correct? And what should we do to pump them up a bit?

Mr. LISCOUSKI. Yes, I think it is fair. I think your characterization of the telecoms and the IT–ISAC as well as others—I think the energy ISAC is another good example, oil and gas. We are looking at them. I guess the easiest answer is that we are examining the best model.

I think currently it is sort of a one-size-fits-all model and it is really not the appropriate one. I think the more we learn about the way information sharing needs to be propagated across the sectors, they are so diverse, many of them are very diverse and not technically connected. We need to look at that more quickly, and we are going through that examination process right now.

Ms. LOFGREN. When will that be completed, do you think?

Mr. LISCOUSKI. You know, completion is probably—I mean, I am really looking at changing the model fairly quickly. The funding model is one of those things. I don't want to give you specific data. I would like to get back to you with more of an intelligent answer about what that is going to look like. I think what I would like to do and what I am planning on doing is actually starting a couple of different types of pilots to see what does work. And I would be happy to share that with you in more detail at a later time when we have pretty much our plans finalized.

Ms. LOFGREN. I would be interested in that, if you could keep us posted. I am sure the whole committee would like to know about it. And if there is a requirement to change the funding stream—I don't know whether we need legislation to do that or not—but I would be interested in that recommendation from you.

Mr. LISCOUSKI. Sure.

Ms. LOFGREN. And additionally, in addition to the functioning of the ISACs, internally I have heard criticism that there is sort of—they are piped, and that there really needs to be some communication among them as well. So I assume that you are—.

Mr. LISCOUSKI. Yes, ma'am, that is precisely the point we are looking.

Ms. LOFGREN. All right. The final question I have has to do with the vacancy rate in your Department. And when you were talking about how challenging it was to come in, I am sure it has been and you want to get good people, you want to get the right people; and it is hard to start an organization from scratch and try and go 65 miles an hour while you are doing it. So I don't want to appear overly critical.

But I am concerned that the vacancy rate is still very high, about 40 percent, I would think. And in a way I have been concerned about this, not just with DHS but other Federal departments when we have tried to get people with expertise and technology to come to work for the Federal Government. I tried with the former commissioner of the INS before the creation of the Department. I mean, we couldn't get people to come to work for the Federal Government, which is disappointing. And especially now with the terrible economic situation in the tech sector, it seems almost mysterious that we can't do a faster, better job of recruiting in this sector.

So the question is: What are you going to do to fill those vacancies? What can we do, if anything, to help you in getting staffed up as quickly as possible?

Mr. LISCOUSKI. Well, I appreciate the concern. And, you know, attrition rates and vacancy rates are things that always plague every business or every government. So it is not a question of that. And I can't speak to the exact number, so I apologize. I mean, we can get back to you on that.

But let me just address it by this. First of all, the workforce we are attracting is a talented workforce. I mean, we are extremely fortunate with some of the folks that we have attracted. And I think, you know, in my experience—I was in the government; I left my career with the State Department back in 1991 And was very impressed with the folks I worked with and my colleagues. I am happy to say I think that workforce has continually increased in its capabilities, particularly in DHS; I have been gratified to see that, folks particularly in the IAIP area. So we have been successful in doing that.

One of the challenges we have when we recruit people from the private sector is going through the clearance process, because the clearance process and working at the levels we are working at require us to take a 6—to 9-month clearance process, and you really can't even work effectively at all until you have got those appropriate clearances. So, while we may have people identified in positions, they can't occupy those positions until they have been vetted and the clearances have granted. And that might be contributing to some of the vacancies you are hearing about.

But we are working hard. And, you know, I appreciate your comments and I would like to just kind of, I guess, recognize that the people that are there today are really working extremely hard. I mean, this country is extremely fortunate, and I have got the benefit of working with them on a daily basis, and they put in some incredible hours and they are really dedicated.

And I can tell you right now, since March 1st, the folks that work in our directorate have been working nonstop. I mean, literally, you go in there on Saturdays and Sundays, and some days you think it is a Wednesday. You know, it is just—it is staffed, And people work hard and they are dedicated. So we are very fortunate.

Ms. LOFGREN. If I can follow up—and that is good to hear. Perhaps the resources that we should apply then might not even be in your Department but in the FBI to—maybe additional resources to do the clearances. Would that be of assistance? I mean, there is no real reason why it has to take 9 months to do the clearances, just the work is the lack of personnel to put on it.

Mr. LISCOUSKI. I am not competent to be able to answer that question, but I suspect we can probably get back to you on that.

Ms. LOFGREN. I would like to know that. And that may be something we could help to address, because that is something we ought to address, it seems to me.

And I yield back my time, Mr. Chairman. Thank you.

Mr. THORNBERRY. I thank the gentlelady.

Dr. Christensen.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman. Mr. Chairman and Ranking Member, it does occur to me, and it came up earlier, that there may be reasons for us to ask the assistant secretary to meet with us in a closed and classified setting, because there may be some questions we might not want to ask in a public hearing.

I have one further question for you, Assistant Secretary. One of the objectives of the National Strategy is to foster adequate training and education programs to support the national security need. You talked about the relationship with Carnegie–Mellon and you made reference to relationships with other universities. I wonder if

you would elaborate on that some, and also talk a bit about how you would ensure the involvement of historically black colleges and universities and other minority-serving institutions.

Mr. LISCOUSKI. Yes, ma'am. There are a couple of different ways we are addressing that. First of all, my colleague, Under Secretary McCreary, has got a program—and forgive me for not knowing the exact specifics on this—in which they are creating partnerships with universities. And I believe it is among those major components that the partnerships are to enhance educational opportunities for the specific areas that we need. So I think it is probably more appropriate to sort of field that question to Under Secretary McCreary's area.

But in our area and working with other partners, you know, the NSA sponsoring the centers of excellence and the university programs that they have, are geared toward enabling opportunity, creating opportunities for educational programs and students to get into the information security area in particular. It is an area that we have a very keen interest in and we are looking to support that.

I can't speak to the programs themselves in terms of where the emphasis is on that program in historically black colleges, but I am almost certain I remember a conversation with NSA officials that they have established centers of excellence at schools that really honor diversity. But, again, I can't speak competently to that question, but I would be happy to get back to you.

Mrs. CHRISTENSEN. Well, given the extensive need for personnel who are really—who are well-skilled and trained, and the sensitivity of the issues that we are going to be dealing with, not allowing us to always go overseas to seek personnel for these offices, I think it is important that we build up our personnel from within and that we extend and expand it to include these institutions as well.

Mr. LISCOUSKI. I agree.

Mrs. CHRISTENSEN. Thank you.

Mr. LISCOUSKI. Thank you.

Mr. THORNBERRY. Ms. Jackson-Lee.

Ms. JACKSON-LEE. Thank you, Mr. Chairman. I again thank you for the hearing that we will have tomorrow and the one that we are having today.

I would like to join Congresswoman Christensen on this issue of HBCUs and the matching of talent. And I think that your point about outreach is extremely important. I would make a suggestion that the Secretary be referred to having a meeting with the president of at least a number of our HBCUs. They are certainly—I think it is definable as to those institutions that may even have those disciplines that would be an excellent feeding source, or a source of talent. And I would add, of course, Hispanic-serving institutions as well. We did that in the previous administration with having a roundtable with about 10 to 20 HBCU presidents, and it really, really is effective in terms of getting them focused and working in partnership with talented individuals who may not be aware of the opportunities and but yet they have great talent.

So I would appreciate it if we could get a response back on that request as to the facilitating of that meeting. And any way that we can help to facilitate would be happy to do so.

Mr. LISCOUSKI. Yes, ma'am, thank you. I think that is a great suggestion. And I can tell you, we would like to take you up on that, but we will get back to you formally.

Ms. JACKSON-LEE. I appreciate it very much.

Mr. LISCOUSKI. Thank you.

Ms. JACKSON-LEE. Let me note, if I understand, when I asked the question about blackout, just give me your answer again. You were saying it is another committee? Or you are going to be here tomorrow discussing? I know we have a hearing tomorrow and we have that as one of our topics. Is that what you were suggesting to me, that you would be able to give more on this issue of what impacts cyber had on the blackout tomorrow? Or are you waiting on a report?

Mr. LISCOUSKI. I may be able to speak at a top level tomorrow; but in earnest, I have to tell you, we have to really conclude the report. We are still going through the analysis. So it is really any preliminary conclusions we come to at this point can easily be eclipsed by other facts that might lead us to a different conclusion. So I will just have to defer to the report, ma'am.

Ms. JACKSON-LEE. And that report will be—what is the date are we looking at for that?

Mr. LISCOUSKI. I don't know if it has been published in terms of the specific dates. I know the task force is shooting for sometime in the late October time frame.

Ms. JACKSON-LEE. Late October.

Mr. LISCOUSKI. Yes, ma'am.

Ms. JACKSON-LEE. And that is, of course, a public report?

Mr. LISCOUSKI. Ma'am, I don't know, to be honest with you. I will have to find out.

Ms. JACKSON-LEE. All right. Well, will you provide us with that information even tomorrow as to the status of that report?

Mr. LISCOUSKI. Certainly.

Ms. JACKSON-LEE. Let me just pursue briefly the line of questioning that I had before about authority and the role of DHS. And I think you said to me that the role is to protect from cyber terrorism; that DHS protects from cyber terrorism, and the FBI is in the business of responding to the attacks or really on the aggressive end of it.

My concern is does it make sense to divide the experts, the ones that are telling us the story, and then those who have to react to the story? Is there a protocol to have two teams, the two teams interact with each other? And then when there is a crisis—that is a question I was asking—who is in charge? Now, you indicated the FBI. But then how does the component that you work with get merged into the FBI? Because when we are in crisis, we need all of the thinkers working together, the reactors; but those who say I have got a solution, because I know on the protection side what we had to do. And a protection response, is it making it more difficult to get people in the protection side? Because certainly there is a lot more energy and excitement maybe on the response side. But I am particularly concerned about the authority question and the protocol that would merge them, if necessary, and whether there is interaction even in the backdrop of the day-to-day work, which I think is extremely important.

Mr. LISCOUSKI. I thank you for the opportunity to clarify, because I think I misled you a bit on my remarks earlier. It is not unique to the FBI in terms of the enforcement and the investigative responsibility. The Secret Service—and, as you know, Secret Service is a component of DHS with whom we closely work—also has a responsibility to investigate cyber crime. In fact, within the financial domain, they are really the preeminent experts.

Ms. JACKSON-LEE. That was a new addition to their responsibilities.

Mr. LISCOUSKI. Yes, ma'am, and they are effectively executing against that. They have some tremendous talent, as does the FBI. We are very ecumenical in our approach. We try to ensure that we have got the right resources. And I think the recent—forgive me, I don't know if it was Blaster or SoBig in which both the FBI and the Secret Service jointly investigated, and they worked extremely well together; they complemented themselves extremely well.

From my point of view, you can never have enough resources to investigate these things. So I think if a little is good, more is better in this case. And the unique capabilities that are within the domain of the Bureau and the FBI I think both complement themselves and overlap where they are necessary; it is appropriate. We work very closely.

And I will just state this: that my intention in creating our capability within IAP and the NCSD is to continuously increase our reliance upon the Secret Service for their capabilities. So, by extension, I would say DHS clearly has the authorities we need. When I was discussing this as it relates to the protection responsibility, it was really relevant to the IAIP mission and the infrastructure protection mission specifically. We do not have investigative authority. We don't need investigative authority, to be candid with you. We have the resources in-house, the DHS, to investigative requirements as we identify them.

Ms. JACKSON-LEE. But you feel you have sufficient authority to work on the matters that you are working on, but also to coordinate with the other agencies when there is a time of crisis?

Mr. LISCOUSKI. Yes, ma'am. In fact, I think we have been able to demonstrate that effectively, as I indicated, through the recent Blaster and SoBig viruses, the blackout. All those incidents have served to really validate the fact that this approach is the appropriate one.

Ms. JACKSON-LEE. Thank you. Thank you, Mr. Chairman.

Mr. THORNBERRY. I thank the gentlelady.

Does Mr. Meek have additional questions?

Mr. MEEK. Just a small one, Mr. Chairman.

Mr. Secretary, I guess we are going to need at a future date—and I don't know, maybe the Chairman and others are thinking about it—but a closed hearing; we can ask a few aggressive questions as it relates to cybersecurity and as it relates to the security of our infrastructure here in the United States.

What level of, would you say, urgency and concern that jointly government and the private sector may have as it relates to a cyber attack? The reason why I ask that question, Mr. Secretary—there may be a quick answer that you can give me—is the fact that we know that there are terrorist groups that are abroad, and possibly

could be domestic, that would like to take our ability to be able to live financially and socially through the Internet. And since we are doing—seems that we are doing a good job as it relates to trying to keep terrorists and track them down before they cross our borders, and using the approach that they are using in Iraq right now of saying why do we have to come to the United States, we can go to Iraq and still accomplish our goal—what kind of urgency do you see? Because I hear a lot of we are fine, we don't need X, Y, and Z, when I know that there are issues out there that need to be addressed and there are issues that this subcommittee needs to address legislatively. There are issues that the Department needs to address rule-wise and administratively. But maybe there are some areas that you feel that are important that we need to fill the gap. And I am just trying to think of the urgency.

I used to be a law enforcement person, and no one is really concerned about the parking lot security outside of any hospital until someone gets pushed down and their wallet or purse is taken. So I am trying to make sure that what—from a scale of 1 to 10, where do you think we are and where do we need to be? Or are we in the right position right now? Everyone, hands on deck, just like they were for the last couple of years? What do you think we need to do here?

Mr. LISCOUSKI. Well, I mean, let me just clarify my statements earlier about where we are. I think we are positioned for success. I think we have got the right architecture, the right framework to build on. I think we know where we have to go. But I did not mean to imply that the world out there is not a bad world.

I agree with you 100 percent; there are some serious threats that we face. The cyber community, the cyber world is one which we are just really beginning to understand and beginning to see the evidence of what those threats can do to manifest themselves in our technologies. So in terms of sense of urgencies, I don't want to sit here calmly explaining to you what we are doing and give you the false perception that I am not worried about it. I am worried about it all the time. And we need to be worried about it. And the community needs to be worried about it, because we are not in control of those threats.

The challenge we have on the cyber world, unlike the physical world where you can really put your arms around somebody and identify the command-and-control structure and the capabilities that they may or may not have to conduct an attack, the cyber world is a lot easier to work in. And although the technologies that you need to do to—there is a debate about how technically savvy you have to be to really conduct a really effective attack or a long sustainable attack. I would argue that I wouldn't want to wait to find that out, and we need to move aggressively and we need to be worried about it.

So I am happy to sit calmly before this committee and talk about the things we are doing. But we are not sitting back calmly back at DHS and other places, just thinking about are we doing the right things. We are really trying to move out and get urgency around this.

So I agree with you and I share that, and I appreciate your comments of concern, because we are concerned about it. These threats

are real, they are ubiquitous, they are everything from the kid that gets bored and decides that he is going to put a virus out there, to organized crime groups that are out there exploiting our networks and exploiting our information and extorting them.

Mr. LISCOUSKI. Terrorist groups, state groups, you name it. They are out there. Common thieves, common criminals. They all have the capabilities of doing these things and doing it all the time. We are constantly under attack on the Internet, and you know, if you talk to any of the providers out there and you talk to the folks who are providing services on the Internet community, the backbone, they see threats all the time. They see stuff, it just would boggle your mind. Fortunately, you know they haven't manifest themselves in anything serious yet. And it is the "yet" that worries me, the ability to do that is out there, so.

Mr. MEEK. Mr. Secretary, if I may, that's where I mean, you are hitting exactly where I thought you would hit as it relates to the threat. And the threat is real. We have individuals that are being robbed right now over the Internet, stuck up, ransom, what have you, $50,000 transferred here and no one will ever know about it because it has a lot to do with stocks and trades and investors and security of their own infrastructure. I just want to make sure that we continue to have a sense of urgency. It is not about the preparedness. It is about the consistency of the preparedness. And I know my job and I know our job is to support the Department and the private sector in its efforts, but at the same time, make sure not only that DHS has what it needs, but we keep the pressure on all players of making sure that we do what we have to do, because the last thing that we want is for you for me or anyone on this committee to be identified as okay. You are okay, I am okay, okay, fine. Everything is fine. We need to make sure that you are okay, I am okay, how do we move this ball and play offense because they are playing offense.

So I am glad to hear that you are still sitting on the edge of your seat personally and that people who serve in your capacity in the private sector has that same sitting on the edge of the seat hopefully as it relates to playing toward overall infrastructure protection. Thank you, Mr. Chairman.

Mr. LISCOUSKI. Thank you.

Mr. THORNBERRY. I thank the gentleman. And I think that discussion that he just had with the witness is an appropriate way to end our hearing because—and I have some additional questions I would like to submit for the record, but I think that sense of urgency that he described is difficult to maintain, not just with cyber, with the whole range of Homeland Security responsibilities. But, yet, we must try to keep that sense of urgency because there is so much at stake. Mr. Liscouski, I will say for me, personally, I am impressed by the actions that you have taken in the cyber field to help bring us closer to where we need to be. I am also convinced that you maintain this sense of urgency.

As you said at the end of your opening statement, we are partners in this effort. That doesn't mean we are a rubber stamp, it doesn't mean we are a cheerleading squad. But we are partners with you to try to help maintain the sense of urgency and take real concrete steps that help our country be safer. We look forward to

working with you in the future to do that. And again, thank you for your appearance today. I thank the gentlelady from California as always for her work and with that the hearing stands adjourned.

[Whereupon, at 11:40 a.m., the subcommittee was adjourned.]