THE DHS CYBERSECURITY MISSION: PROMOTING INNOVATION AND SECURING CRITICAL INFRASTRUCTURE

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

APRIL 15, 2011

Serial No. 112–19

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PRINTING OFFICE
72–229 PDF WASHINGTON : 2012

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

COMMITTEE ON HOMELAND SECURITY

Peter T. King, New York, *Chairman*

Lamar Smith, Texas
Daniel E. Lungren, California
Mike Rogers, Alabama
Michael T. McCaul, Texas
Gus M. Bilirakis, Florida
Paul C. Broun, Georgia
Candice S. Miller, Michigan
Tim Walberg, Michigan
Chip Cravaack, Minnesota
Joe Walsh, Illinois
Patrick Meehan, Pennsylvania
Ben Quayle, Arizona
Scott Rigell, Virginia
Billy Long, Missouri
Jeff Duncan, South Carolina
Tom Marino, Pennsylvania
Blake Farenthold, Texas
Mo Brooks, Alabama

Bennie G. Thompson, Mississippi
Loretta Sanchez, California
Sheila Jackson Lee, Texas
Henry Cuellar, Texas
Yvette D. Clarke, New York
Laura Richardson, California
Danny K. Davis, Illinois
Brian Higgins, New York
Jackie Speier, California
Cedric L. Richmond, Louisiana
Hansen Clarke, Michigan
William R. Keating, Massachusetts
Vacancy
Vacancy

Michael J. Russell, *Staff Director/Chief Counsel*
Michael S. Twinchek, *Chief Clerk*
I. Lanier Avant, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

Daniel E. Lungren, California, *Chairman*

Michael T. McCaul, Texas
Tim Walberg, Michigan, *Vice Chair*
Patrick Meehan, Pennsylvania
Billy Long, Missouri
Tom Marino, Pennsylvania
Peter T. King, New York *(Ex Officio)*

Yvette D. Clarke, New York
Laura Richardson, California
Cedric L. Richmond, Louisiana
William R. Keating, Massachusetts
Bennie G. Thompson, Mississippi *(Ex Officio)*

Coley C. O'Brien, *Staff Director*
Alan Carroll, *Subcommittee Clerk*
Dr. Chris Beck, *Minority Subcommittee Director*

CONTENTS

Page

STATEMENTS

WITNESSES

THE DHS CYBERSECURITY MISSION: PROMOTING INNOVATION AND SECURING CRITICAL INFRASTRUCTURE

Friday, April 15, 2011

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE
PROTECTION, AND SECURITY TECHNOLOGIES,
Washington, DC.

The subcommittee met, pursuant to call, at 10:08 a.m., in Room 311, Cannon House Office Building, Hon. Daniel E. Lungren [Chairman of the subcommittee] presiding.

Present: Representatives Lungren, McCaul, Meehan, Marino, Clarke, and Richardson.

Mr. LUNGREN. The Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will come to order.

I apologize for being a few minutes late. We had a special Republican Conference.

We are supposed to have votes at 10:15 and then at 11:15 and then at 12:15. So we will be bopping back and forth between those. Actually, they are single votes, I think, so we can come right back after that. So I apologize to our panel.

We have had a slightly different schedule so that we would not have interrupted hearings, but today is a little bit of a different day. We are only going to vote on visions of the budget for this coming year and the next 10 years, and this week we get to talk about trillions instead of billions. So it is just small votes that we have got today. I am sorry that that will take us away, but I do thank you for being here.

Today, the subcommittee will examine the relationship between the Department of Homeland Security and the owners and operators of critical infrastructure. What is working well, what could be done better, and how to improve in the future.

So we are meeting today to hear testimony from Seán McGurk, the Director of National Cybersecurity and Communications Integration Center, or NCCIC—once we start with all these initials, it gets confusing, so I will try to stay away from that as much as possible—Gerry Cauley, President and CEO of North American Electric Reliability Corporation; Jane Carlin, Chair of the Financial Services Sector Coordinating Council; and Dr. Edward Amoroso, the Senior Vice President and CSO of AT&T.

This is an important hearing, so important I had a nice long statement. But because of the time that we have, I will have my statement entered for the record and recognize my Ranking Minority Member of the subcommittee, the gentlelady from New York, Ms. Clarke, for any statement she may have.

[The statement of Mr. Lungren follows:]

PREPARED STATEMENT OF CHAIRMAN DANIEL E. LUNGREN

APRIL 15, 2011

Welcome to the second in our series of cybersecurity hearings. Today's hearing will focus on "the Department of Homeland Security's Cybersecurity Mission."

Homeland Security Presidential Directive 7, issued on December 17, 2003 outlines our National policy for Federal departments and agencies to partner with the private sector to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. The Secretary of Homeland Security was given the responsibility for "coordinating the overall National effort to enhance the protection of the critical infrastructure," whether owned and operated by the public or private sector. With the private sector owning more than 80% of the Nation's critical infrastructure, the DHS-Private Sector relationship is crucial.

As stated in our previous subcommittee hearing on March 16, information networks and computer systems face a combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and a lack of comprehensive threat and vulnerability awareness. A successful attack on our power grid or our communications networks could not only cripple our economy but threaten our National security.

Under current law the vast majority of critical infrastructure fall outside the Department's direct cybersecurity regulatory authority. Under the Homeland Security Act of 2002, the Department was authorized to provide, upon request, analysis and warnings related to threats and crises management support to private sector owners and operators of critical information systems. They can also provide technical assistance to the private sector with respect to emergency recovery plans when responding to major failures of critical information systems. The Department does not have the ability to require the private sector use of any particular cybersecurity processes or tools. In this environment of ever-changing technology and innovation, I believe this is sound policy.

It is important to note that just because the Department can not directly regulate the cybersecurity requirements of various sectors that the private sector is completely unregulated. The electric power sector has had mandatory cybersecurity standards in place since 2008 and Sarbanes Oxley Act requires all publically traded companies certify that they have proper internal controls in place on their financial accounting systems. This requirement, in essence, equates to requiring proper cybersecurity in their IT/Finance systems.

Without direct regulatory authority, the Department exercises much of its responsibility for securing private critical infrastructure as a coordinating agent. The Department has established a number of cybersecurity functions and services to help in its role as coordinator. The National Cybersecurity and Communications Integration Center (NCCIC) enables the Department to bring together its Federal partners as well as members of the private sector to integrate information and provide the focus of cybersecurity operations for the entire Federal Government. I was privileged to be invited to the ribbon-cutting ceremony for this cybersecurity and communications integration center which we all hope will become the model for a successful public-private cybersecurity partnership.

The public-private partnership remains a key part of the Nation's efforts to secure and protect its critical cyber-reliant infrastructure. While criticized by some, it is still evolving since its inception a decade ago. Because of the leadership of NPPD Under Secretary Rand Beers and Deputy Secretary Phillip Reitinger, the Department has strategically positioned cybersecurity resources and assets in an effort to develop a more trusted and mutually beneficial public-private partnership that is needed to defend cyberspace. Without ownership, partnership is the next best thing for promoting cybersecurity and protecting our critical infrastructure. If properly developed and implemented, the public-private partnership cybersecurity model can be leveraged to improve the culture of security and the willingness of the private sector to make the necessary investments to secure their critical infrastructure.

With all this cyber expertise, is the Department making a real difference in defending critical infrastructure? Are they protecting Government and private sector cyber space and responding effectively to cyber attacks? Are they assisting the private sector in detecting, defending, and recovering from cyber attack? Is the Department making available to its partners the critical threat information they need to protect their networks?

Today we will hear from the Homeland Security Department and a number of key economic sectors, whose critical infrastructure is vital to maintaining our robust economy, on how this public-private partnership is progressing.

I now recognize the Ranking Member Ms. Clarke for her opening statement.

Ms. CLARKE. Thank you very much.

Good morning and thanks to all of our witnesses for appearing before us today. I would like to thank you, Chairman Lungren, for holding our second hearing on cybersecurity this session and for your intention to move expeditiously on what I know we both recognize as a critical issue. I know Mr. Lungren takes this responsibility as seriously as I do, and I look forward to partnering with him again over these 2 years to ensure the safety and security of the American people, American businesses, American infrastructure, and the American way of life.

Today's hearing will focus on our critical infrastructure sectors, their cybersecurity posture, and the DHS role in helping them to be as secure and simultaneously as open and as efficient as possible.

We rely on information technology in every aspect of our lives, from our electric grid, financial and communication systems, and Government functions, to name just a few that our witnesses here today represent. Interconnected computers and networks have led to amazing developments in our society. Increased productivity, knowledge, services, and revenues are all benefits generated by our modern, networked world.

But in our rush to network everything, few stop to consider the security ramifications of this new world we are creating; and so we find ourselves in a very vulnerable situation today. As I stated at our last hearing, too many vulnerabilities exist on too many critical networks which are exposed to too many skilled attackers who can steal from or damage too many of our systems. Unfortunately, to this day, too few people are even aware of these dangers, and fewer still are doing anything about it.

This committee will continue to discuss and examine these issues in an attempt to raise awareness of the problems we face, and we hope to identify and implement practical and effective solutions. There is a very real and significant threat to our National and economic security that we now face in cyberspace, and we must do something equally real and significant to meet this challenge.

As I noted at our hearing last month, we are expecting that this committee is eager to see a National cybersecurity strategy from the White House to be released very soon. I also stated at our last hearing that the Department is finalizing its National security incident response plan and will also include a cybersecurity strategy, as called for in the 2010 Quadrennial Homeland Security Review.

Mr. McGurk I hope to hear some good news from you on these items, because we can't keep waiting for these things. The Congress is interested in moving legislation to afford DHS the authority it needs to protect the dot-gov domain and critical infrastructures in the private sectors. Hopefully, we are downplaying these

Government shutdown games here in Congress, and we will get on to the business that our constituents elected us to do.

This cybersecurity issue is complicated, and no one entity or approach will work. I firmly believe that the U.S. Government and the private sector must be full partners in this effort; and both must accept their share of burden, responsibility, and cost of our combined security.

The intention behind this hearing is to focus on the protection of the critical infrastructures that sustain our lives and our economy. These infrastructures are under constant attack. Cybercrime alone costs this country billions of dollars a year. We know that our Government networks are attacked tens of thousands of times per day, and private sector networks are attacked even more often. We know that our critical infrastructures are already compromised and penetrated. We need to absorb this information, get up to speed quickly, and move forward to address this issue. We have to start protecting ourselves before an attack big enough to cause irreparable damage is carried out.

To the witnesses appearing before us today, I thank you for being here, and I welcome your thoughts on the issues before us, including what you think an effective National cybersecurity policy should look like and especially the critical details needed to make this public-private partnership work. Chairman Lungren and I intend for this subcommittee as well as the full committee to play a leading role in shaping our National cyber posture in the years to come.

Finally, I would like to thank Dr. Chris Beck for his hard work on behalf of this subcommittee. Dr. Beck has worked tirelessly on chemical security legislation. He will be leaving the subcommittee and will be missed.

Thank you, Mr. Chairman; and I yield back.

Mr. LUNGREN. Thank you very much.

I appreciate the comments, and I would echo the statements that you made about Dr. Beck. I know he will still be around in town, and we will be able to see him.

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

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

Seán McGurk has over 32 years of experience in advanced systems operations and information systems security. He joined DHS in 2008 after a full career in the Navy. He was named Director of the Control System Security Program and led the Industrial Control Systems Computer Emergency Response Team prior to leading NCCIC. NCCIC is a 24-by-7 integrated cybersecurity and communications operation center, providing indications and warnings of incidents through cross-domain situational awareness. It is a hub of information sharing amongst various Government agencies as well as private-sector stakeholders.

Gerry Cauley is President and Chief Executive Officer of the North American Electric Reliability Corporation. Previously, he served as President and Chief Executive Officer of the SERC Reliability Corporation, a nonprofit corporation responsible for promoting and assessing the reliability and critical infrastructure protection of the bulk power system in 16 southeastern and central States.

Prior to that, Mr. Cauley worked for NERC for 10 years in positions of increasing responsibility, ultimately as Vice President and Director of Standards. He was instrumental in preparing NERC's application to become the electric reliability organization and spearheaded their development of an initial set of standards to ensure the reliability of the bulk power system in North America.

He is also a lead investigator of the August, 2003, northeast blackout and coordinated all aspects of the NERC Y2K program, supervising the reporting and readiness of 3,100 electric organizations in the United States and Canada.

Jane D. Carlin, Chair of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. But in her spare time she is Managing Director of Morgan Stanley and Global Head of Operational Risk Management, Business Continuity, Information Security, and Risk and Insurance Management.

Ms. Carlin has concentrated on legal and risk issues in banking and investment banking related to international and domestic securities, derivatives, and commodities as well as foreign exchange. She received her J.D. from Benjamin Cardoza School of Law and her B.A. from the State University of New York at Stony Brook.

Dr. Edward Amoroso is presently Senior Vice President and Chief Security Officer for AT&T, where he is directly responsible for managing the day-to-day information, computer, and network security protection of AT&T's vast global infrastructure. He and his team of security engineers, developers, researchers, and consultants design and manage all security policy, security regulatory issues, scanning, firewall, intrusion detection, data fusion, antivirus, anti-spam, instant response, emergency response, and other protection systems for the corporation and its customers. He also directs the design and development of AT&T's rich portfolio of managed and customized security services for business and Government clients.

We would ask each of you to try to limit your remarks to about 5 minutes. We have your prepared remarks. They will be entered in as a part of the record.

As I say, we probably will have to break and go and vote and then come back. I am going to see if we can get the opening statements finished before we have to go vote.

So, Mr. McGurk, you are asked to please give us your best shot for 5 minutes.

STATEMENT OF SEÁN MCGURK, DIRECTOR, NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER, DEPARTMENT OF HOMELAND SECURITY

Mr. McGurk. Thank you Chairman Lungren, Ranking Member Clarke, and distinguished Members of the committee. My name is Seán McGurk, and I thank you for those kind opening words and introduction.

I also thank you for inviting me to be part of this very distinguished panel of experts to discuss the challenges associated with innovation and securing critical infrastructure.

Recently, Deputy Under Secretary Reitinger testified before this panel, and the Department greatly appreciates the support and the guidance that we have been receiving in completing our essential mission.

As several of the distinguished Members of the committee have already mentioned, the cyber environment is not a homogenous environment under a single department, agency, or private-sector entity. The National Infrastructure Protection Plan identifies the 18 sectors of the critical infrastructure, each being unique and diverse. In fact, in many facilities, two operating plants under the same control of an organization have completely different network environments. We rely on these continuously available services for our vast way of life and the interconnected critical infrastructure to sustain those. Successful cyberattacks against these systems could potentially result in a physical damage or loss of life.

We face many challenges—strong and rapidly expanding adversary capabilities, a lack of comprehensive threat and vulnerability awareness—and in these efforts we must support our private-sector partners in securing the systems and themselves against these malicious activities.

The Government does not have all the answers, so we must work closely with the private sector to ensure that we have identified the vulnerabilities and the risks to the critical infrastructure. There is no one size fits all. There is no cyber Maginot Line that will enable us to provide security across the board.

What I have learned in my experience both in the United States Navy and as a member of the Department in over 34 years, it is not all about 10-pound brains or bigger guards, gates, and guns that gets the job done. It is about involving a very broad audience and sharing information and building a collective body of knowledge. We must leverage the Government's expertise and our access to information, including classified data, along with industry-specific needs, capabilities, and timelines. Each partner has a role to play and a unique capability that adds value to the team.

In a recent example involving two-factor authentication, we worked closely with our law enforcement partners to identify and hopefully potentially prosecute those responsible. We worked with the intelligence community and the military to attribute the activity and also to provide defensive capability and potential pursuit.

The Department of Homeland Security's primary focus is on mitigation and risk protection of systems, working closely with the private sector. In this particular example, we have representatives from the financial sector, the communications sector, the energy sector, and the IT sector working on a broad mitigation strategy to aggressively address those challenges. We are looking to prepare, prevent, respond, recover, and restore in the Department's role.

Coordinating a National response under the National cyber incident response plan enables us to bring these private-sector partners to the table and their subject matter expertise to determine the "what" and the "how" to protect these networks and not necessarily worry about the "who" and the "why" until much later.

The NCCIC closely works with all Government agencies and the private sector through our partnership model. We have representatives from the Communications Information Sharing and Analysis

Center, along with companies such as AT&T. The IT, ISAC, and the financial services sector are all physically represented on the watch floor. We are finalizing our agreement with the North American Electric Reliability Corporation and the energy sector ISAC to have full-time support on the watch floor as well.

In addition, working with our State, local, Tribal, and territorial partners through the multi-State Information Sharing and Analysis Center, we can virtually reach out to each of the States and localities to ensure that they are fully aware of the cyber vulnerabilities and risk mitigation strategies that are being developed.

In conclusion, within our current legal authorities we continue to engage, collaborate, and provide analysis, vulnerability, and mitigation assistance to the private sector. We have the experience and the expertise in dealing with the private sector in planning steady state and crisis scenarios. In support of that we deploy numerous incident response and assessment teams that enable us to help prevent, prepare, and recover from these cyber impacts.

Finally, we work closely with the private sector and our interagency partners in law enforcement and intelligence to provide a full complement and capabilities for preparation for and in response to significant cyber events.

Chairman Lungren, Ranking Member Clarke, and distinguished Members of the subcommittee, let me conclude in reiterating that I look forward to exploring the opportunities to support this mission and collaborate with the subcommittee and my colleagues in the public and private sectors.

Thank you again for this opportunity, and I would be happy to stand by and answer any of your questions.

[The statement of Mr. McGurk follows:]

Prepared Statement Seán P. McGurk

April 15, 2011

INTRODUCTION

Chairman Lungren, Vice Chairman Walberg, Ranking Member Clarke, and distinguished Members of the subcommittee, it is a pleasure to appear before you today to discuss the Department of Homeland Security's (DHS) cybersecurity mission. Specifically, I will discuss the Department's cybersecurity mission as it relates to critical infrastructure and our coordination of this mission with the private sector.

Deputy Under Secretary Philip Reitinger recently testified before this subcommittee, and I would like to reiterate the Department's desire to work more with you to convey the relevance of cybersecurity to average Americans. Increasingly, the services we rely on in our daily life, such as water distribution and treatment, electricity generation and transmission, health care, transportation, and financial transactions depend on an underlying information technology and communications infrastructure. Cyber threats put the availability and security of these and other services at risk.

THE CURRENT CYBERSECURITY ENVIRONMENT

The United States faces a combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and a lack of comprehensive threat and vulnerability awareness. Within this dynamic environment, we are confronted with threats that are more targeted, more sophisticated, and more serious.

Sensitive information is routinely stolen from both Government and private sector networks, undermining confidence in our information systems and the sharing of information. As bad as the loss of precious National intellectual capital is, we increasingly face threats that are even greater. We face threats that could significantly compromise the accessibility and reliability of our information infrastructure.

Malicious actors in cyberspace, including nation states, terrorist networks, organized criminal groups, and individuals located here in the United States, have varying levels of access and technical sophistication, but all have nefarious intent. Several are capable of targeting elements of the U.S. information infrastructure to disrupt, or destroy systems upon which we depend. Motives include intelligence collection, intellectual property or monetary theft, or disruption of commercial activities, among others. Criminal elements continue to show increasing levels of sophistication in their technical and targeting capabilities and have shown a willingness to sell these capabilities on the underground market. In addition, terrorist groups and their sympathizers have expressed interest in using cyberspace to target and harm the United States and its citizens. While some have commented on terrorists' own lack of technical abilities, the availability of technical tools for purchase and use remains a potential threat.

Malicious cyber activity can instantaneously result in virtual or physical consequences that threaten National and economic security, critical infrastructure, public health and welfare. Similarly, stealthy intruders can lay a hidden foundation for future exploitation or attack, which they can then execute at their leisure—and at their time of greatest advantage. Securing cyberspace requires a layered security approach across the public and private sectors.

We need to support the efforts of our private sector partners to secure themselves against malicious activity in cyberspace. Collaboratively, public and private sector partners must use our knowledge of information technology systems and their interdependencies to prepare to respond should defensive efforts fail. This is a serious challenge, and DHS is continually making strides to improve the Nation's overall operational posture and policy efforts.

CYBERSECURITY MISSION

No single technology—or single Government entity—alone can overcome the cybersecurity challenges our Nation faces. Consequently, the public and private sectors must work collaboratively. Cybersecurity must start with informed users taking necessary precautions and extend through a coordinated effort among the private sector, including critical infrastructure owners and operators, and the extensive expertise that lies across coordinated Government entities. In addition to leading the effort to secure Federal Executive Branch civilian departments and agencies' unclassified networks, the National Protection and Programs Directorate (NPPD) within DHS is responsible for the following key cybersecurity missions:

- Providing technical expertise to the private sector and critical infrastructure and key resources (CIKR) owners and operators—whether private sector, State, or municipality-owned—to bolster their cybersecurity preparedness, risk assessment, mitigation and incident response capabilities;
- Raising cybersecurity awareness among the general public; and
- Coordinating the National response to domestic cyber emergencies.

In a reflection of the bipartisan nature with which the Federal Government continues to approach cybersecurity, President Obama determined that the Comprehensive National Cybersecurity Initiative (CNCI) and its associated activities should continue to evolve as key elements of the broader National cybersecurity efforts. These CNCI initiatives play a central role in achieving many of the key recommendations of the President's *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* Following the publication of those recommendations in May 2009, DHS and its components developed a long-range vision of cybersecurity for the Department and the Nation's homeland security enterprise, which is encapsulated in the Quadrennial Homeland Security Review (QHSR). The QHSR provides an overarching framework for the Department and defines our key priorities and goals. One of the five priority areas detailed in the QHSR is safeguarding and securing cyberspace. Within the cybersecurity mission area, the QHSR identifies two overarching goals: To help create a safe, secure, and resilient cyber environment and to promote cybersecurity knowledge and innovation.

In alignment with the QHSR, Secretary Napolitano consolidated many of the Department's cybersecurity efforts under NPPD. The Office of Cybersecurity and Communications (CS&C), a component of NPPD, focuses on reducing risk to the communications and information technology infrastructures and the sectors that depend upon them, as well as enabling timely response and recovery of these infrastructures under all circumstances. The functions and mission of the National Cybersecurity Center (NCSC) are now supported by CS&C. These functions include coordinating operations among the six largest Federal cyber centers. CS&C also coordinates National security and emergency preparedness communications planning and provisioning for the Federal Government and other stakeholders. CS&C comprises three divisions: The National Cyber Security Division (NCSD), the Office of Emergency Communications, and the National Communications System. It also houses the National Cybersecurity and Communications Integration Center (NCCIC)—DHS' 24-hour cyber and communications watch and warning center. Within NCSD, the United States Computer Emergency Readiness Team (US–CERT) is working more closely than ever with our public and private sector partners to share what we learn from EINSTEIN 2, a Federal executive agency computer network intrusion detection system, to deepen our collective understanding, identify threats collaboratively, and develop effective security responses. EINSTEIN enables us to respond to warnings and other indicators of operational cyber attacks, and we have many examples showing that this program investment has paid for itself several times over.

Teamwork—ranging from intra-agency to international collaboration—is essential to securing cyberspace. Together, we can leverage resources, personnel, and skill sets that are needed to achieve a more secure and reliable cyberspace. Although DHS leads significant cybersecurity mission activities in the public sector, I will focus the rest of my testimony on private sector coordination.

The NCCIC works closely with Government at all levels and with the private sector to coordinate the integrated and unified response to cyber and communications incidents impacting homeland security. Numerous DHS components, including US–CERT, the Industrial Control Systems Cyber Emergency Response Team (ICS–CERT), and the National Coordinating Center for Telecommunications, are collocated in the NCCIC. Also present in the NCCIC are other Federal partners, such as the Department of Defense (DoD) and members of the law enforcement and intelligence communities. The NCCIC also physically collocates Federal staff with private sector and non-governmental partners. Currently, representatives from the Information Technology and Communications Sectors and the Multi-State Information Sharing and Analysis Center are located on the NCCIC watch floor. We are also finalizing steps to add representatives from the Banking and Finance Sector, as well as the Energy Sector.

By leveraging the integrated operational capabilities of its member organizations, the NCCIC serves as an "always on" cyber incident response and management center, providing indications and warning of imminent incidents, and maintaining a national cyber "common operating picture." This facilitates situational awareness among all partner organizations, and also creates a repository of all reported vulnerability, intrusion, incident, and mitigation activities. The NCCIC also serves as a National point of integration for cyber expertise and collaboration, particularly when developing guidance to mitigate risks and resolve incidents. Finally, the unique and integrated nature of the NCCIC allows for a scalable and flexible coordination with all interagency and private sector staff during steady-state operations, in order to strengthen relationships and solidify procedures as well as effectively incorporate partners as needed during incidents.

NCSD collaborates with private sector stakeholders to conduct risk assessments and mitigate vulnerabilities and threats to information technology assets and activities affecting the operation of private sector critical infrastructures. NCSD also provides cyber threat and vulnerability analysis, early warning, incident response assistance, and exercise opportunities for private sector constituents. To that end, NCSD carries out the majority of DHS' non-law enforcement cybersecurity responsibilities.

NATIONAL CYBER INCIDENT RESPONSE

The President's *Cyberspace Policy Review* called for "a comprehensive framework to facilitate coordinated responses by government, the private sector, and allies to a significant cyber incident." DHS coordinated the interagency, State and local government, and private sector working group that developed the National Cyber Incident Response Plan (NCIRP). The NCIRP provides a framework for effective incident response capabilities and coordination among Federal agencies, State and local governments, the private sector, and international partners during significant cyber incidents. It is designed to be flexible and adaptable to allow synchronization of response activities across jurisdictional lines. In September 2010, DHS hosted Cyber Storm III, a response exercise in which members of the domestic and international cyber incident response community addressed the scenario of a coordinated cyber event. During the event, the NCIRP was activated and its incident response framework was tested. Based on observations from the exercise, the plan is in its final stages of revision prior to publication. Cyber Storm III also tested the NCCIC and the Federal Government's full suite of cybersecurity response capabilities.

PROVIDING TECHNICAL OPERATIONAL EXPERTISE TO THE PRIVATE SECTOR

DHS has significant cybersecurity capabilities, and we are using those capabilities to great effect as we work collaboratively with the private sector to protect the Nation's CIKR. We engage with the private sector on a voluntary basis to provide on-site analysis, mitigation support, and assessment assistance. Over the past year, we have repeatedly demonstrated our ability to materially and expeditiously assist companies with cyber intrusion mitigation and incident response. We are able to do so through our trusted and close relationships with private sector companies as well as Federal departments and agencies. Finally, our success in assisting the private sector is due in no small part to our dedication to properly and fully addressing privacy, civil rights, and civil liberties in all that we do. Initiating technical assistance with a private company to provide analysis and mitigation advice is a sensitive endeavor—one that requires trust and strict confidentiality. Within our analysis and warning mission space, DHS has a proven ability to provide that level of trust and confidence in the engagement. Our efforts are unique among Federal agencies' capabilities in that DHS focuses on civilian computer network defense and protection rather than law enforcement, military, or intelligence functions. DHS engages to mitigate the threat to the network to reduce future risks.

Our approach requires vigilance and a voluntary public/private partnership. We are continuing to build our capabilities and relationships because the cyber threat trends are more sophisticated and frequent.

Over the past year, we established the NCCIC and are adding staff to that center, both from existing DHS personnel and from partner organizations in the public and private sectors. More broadly, we are continuing to hire more cybersecurity professionals and increasing training availability to our employees. The NCIRP is operational, and we continue to update and improve it with input from senior cybersecurity leaders. We will be releasing the NCIRP publicly in the near future. We are executing within our current mission and authorities now, receiving and responding to substantial netflow data from our intrusion detection technologies deployed to our Federal partners, and leveraging that data to provide early warnings and indicators across Government and industry. With our people, processes, and technology, we stand ready to execute the responsibilities of the future.

In addition to specific mitigation work we conduct with individual companies and sectors, DHS looks at the interdependencies across critical infrastructure sectors for a holistic approach to providing our cyber expertise. For example, the Electric, Nuclear, Water, Transportation, and Communications Sectors support functions across all levels of government including Federal, State, local, and Tribal governments, and the private sector. Government bodies and organizations do not inherently produce these services and must rely on private sector organizations, just as other businesses and private citizens do. Therefore, an event impacting control systems has potential implications at all these levels, and could also have cascading effects upon all 18 sectors. For example, Water and Wastewater Treatment, Chemical, and Transportation sectors depend on the Energy Sector, and failure in one of these sectors could subsequently affect Government and private sector operations.

US–CERT also collaborates, provides remote and on-site response support, and shares information with Federal, State, and local governments; critical infrastructure owners and operators; and international partners to address cyber threats and develop effective security responses.

DHS provides on-site and remote incident response assistance to its public and private sector partners. Upon notification of a cyber incident, ICS–CERT and/or US–CERT can perform a preliminary diagnosis to determine the extent of the compromise. At the partner's request and when appropriate, either ICS–CERT or US–CERT can deploy a team to meet with the affected organization to review network topology, identify infected systems, create image files of hard drives for analysis, and collect other data as needed to perform thorough follow-on analysis. Both ICS–CERT and US–CERT can provide mitigation strategies, advise asset owners and operators on their efforts to restore service, and provide recommendations for improving overall network and control systems security.

An incident in early 2010 illustrates the incident response support that DHS provides. In this case, an employee of a company had attended an industry event and used an instructor's flash drive to download presentation materials to the company's laptop. The flash drive was infected with the Mariposa botnet, unbeknownst to the event organizer. When the employee returned to the work location and used the laptop, the virus quickly spread to nearly 100 systems. US–CERT and ICS–CERT had already been tracking a trend of removable media involved in malware infections, and, on request, deployed a team to the company's location to help diagnose the malware and identify those infected systems.

The team spent 2 days with the company reviewing the incident details, network topology, and the company's control systems architecture to identify systems of interest. The company was ultimately able to leverage all of the information to contain the infection and remove the malware from the infected systems. ICS–CERT and US–CERT provided follow-on reporting, mitigation measures, and access to additional resources through the US–CERT secure portal.

US–CERT's operations are complemented in the arena of industrial control systems by ICS–CERT. The term "control system" encompasses several types of systems, including Supervisory Control and Data Acquisition, process control, and other automated systems that are found in the industrial sectors and critical infrastructure. These systems are used to operate physical processes that produce the goods and services that we rely upon, such as energy, drinking water, emergency services, transportation, postal and shipping, and public health. Control systems security is particularly important because of the inherent interconnectedness of the CIKR sectors and their dependence on one another.

As such, assessing risk and effectively securing industrial control systems are vital to maintaining our Nation's strategic interests, public safety, and economic well-being. A successful cyber attack on a control system could result in physical damage, loss of life, and cascading effects that could disrupt services. DHS recognizes that the protection and security of control systems is essential to the Nation's overarching security and economy. In this context, as an example of many related initiatives and activities, DHS—in coordination with the Department of Commerce's National Institute of Standards and Technology (NIST), the Department of Energy, and DoD—has provided a forum for researchers, subject matter experts and practitioners dealing with cyber-physical systems security to assess the current state of the art, identify challenges, and provide input to developing strategies for addressing these challenges. Specific infrastructure sectors considered include energy, chemical, transportation, water and wastewater treatment, health care and public health, and commercial facilities. A 2010 published report of findings and recommendations is available upon request.

An additional real-world threat emerged last year that significantly changed the landscape of targeted cyber attacks on industrial control systems. Malicious code, dubbed Stuxnet, was detected in July 2010. DHS analysis concluded that this highly complex computer worm was the first of its kind, written to specifically target mission-critical control systems running a specific combination of software and hardware.

ICS–CERT analyzed the code and coordinated actions with critical infrastructure asset owners and operators, Federal partners, and Information Sharing and Analysis Centers. Our analysis quickly uncovered that sophisticated malware of this type potentially has the ability to gain access to, steal detailed proprietary information from, and manipulate the systems that operate mission-critical processes within the Nation's infrastructure. In other words, this code can automatically enter a system, steal the formula for the product being manufactured, alter the ingredients being mixed in the product, and indicate to the operator and the operator's anti-virus software that everything is functioning normally.

To combat this threat, ICS–CERT has been actively analyzing and reporting on Stuxnet since it was first detected in July 2010. To date, ICS–CERT has briefed dozens of Government and industry organizations and released multiple advisories and updates to the industrial control systems community describing steps for detecting an infection and mitigating the threat. As always, our goal is to balance the need for public information sharing while protecting the information that malicious actors may exploit. DHS provided the alerts in accordance with its responsible disclosure processes.

The purpose and function for responsible disclosure is to ensure that DHS executes its mission of mitigating risk to critical infrastructure, not necessarily to be the first to publish on a given threat. For example, ICS–CERT's purpose in conducting the Stuxnet analysis was to ensure that DHS understood the extent of the risks so that they could be mitigated. After conducting in-depth malware analysis and developing mitigation steps, we were able to release actionable information that benefited our private sector partners.

Looking ahead, the Department is concerned that attackers could use the increasingly public information about the code to develop variants targeted at broader installations of programmable equipment in control systems. Copies of the Stuxnet code, in various different iterations, have been publicly available for some time now. ICS–CERT and the NCCIC remain vigilant and continue analysis and mitigation efforts of any derivative malware.

ICS–CERT will continue to work with the industrial control systems community to investigate these and other threats through malicious code and digital media analysis, on-site incident response activities, and information sharing and partnerships.

INTERAGENCY AND PUBLIC-PRIVATE COORDINATION

Overcoming new cybersecurity challenges requires a coordinated and focused approach to better secure the Nation's information and communications infrastructures. President Obama's *Cyberspace Policy Review* reaffirms cybersecurity's significance to the Nation's economy and security. Establishment of a White House Cybersecurity Coordinator position solidified the priority the administration places on improving cybersecurity.

No single agency has sole responsibility for securing cyberspace, and the success of our cybersecurity mission relies on effective communication and critical partnerships. Many Government players have complementary roles as well as unique capabilities—including DHS, the intelligence community, DoD, the Department of Justice, the Department of State, and other Federal agencies—and they require coordination and leadership to ensure effective and efficient execution of our collective cyber missions. The creation of a senior-level cyber position within the White House ensures coordination and collaboration across Government agencies.

Private industry owns and operates the vast majority of the Nation's critical infrastructure and cyber networks. Consequently, the private sector plays an important role in cybersecurity, and DHS has initiated several pilot programs to promote public-private sector collaboration. In its engagement with the private sector, DHS recognizes the need to avoid technology prescription and to support innovation that enhances critical infrastructure cybersecurity. DHS, through the National Infrastructure Protection Plan partnership framework, has many years of experience in private sector collaboration, leveraging our relationships in both the physical and cybersecurity protection areas. For example, the Office of Infrastructure Protection and the National Cyber Security Division partnered with the chemical industry to publish the *Roadmap to Secure Industrial Control Systems in the Chemical Sector* in 2009, available at *www.us-cert.gov.* To meet the first set of milestones set forth in this 10-year plan, industry, in partnership with DHS, developed a suite of control systems security awareness materials that will be shared widely within the Chemical Sector this summer.

DHS engages with the private sector on a voluntary basis in accordance with our responsibilities under the Homeland Security Act. We stand by to assist our private sector partners upon their request, and thus far have been able to do so successfully due to our technical capabilities, existing private sector relationships, and expertise in matters relating to privacy and civil rights and civil liberties.

In February 2010, DHS, DoD, and the Financial Services Information Sharing and Analysis Center (FS–ISAC) launched a pilot designed to help protect key critical networks and infrastructure within the financial services sector by sharing actionable, sensitive information. Based on lessons learned from the pilot, DHS is developing comprehensive information-sharing and incident response coordination processes with CIKR sectors, leveraging capabilities from within DHS and across the response community, through the NCCIC.

In June 2010, DHS implemented the Cybersecurity Partner Local Access Plan, which allows security-cleared owners and operators of CIKR, as well as State technology officials and law enforcement officials, to access secret-level cybersecurity information and video teleconference calls via State and major urban area fusion centers. In November 2010, DHS signed an agreement with the Information Technology Information Sharing and Analysis Center (IT–ISAC) to embed a full-time IT–ISAC analyst and liaison to DHS at the NCCIC, part of the on-going effort to collocate private sector representatives alongside Federal and State government counterparts. The IT–ISAC consists of information technology stakeholders from the private sector and facilitates cooperation among members to identify sector-specific vulnerabilities and risk mitigation strategies.

In July 2010, DHS worked extensively with the White House on the publication of a draft *National Strategy for Trusted Identities in Cyberspace,* which seeks to secure the digital identities of individuals, organizations, services, and devices during on-line transactions, as well as the infrastructure supporting the transaction. The final strategy is set to be released in the near future, fulfilling one of the near-term action items of the President's Cyberspace Policy Review. The strategy is based on public-private partnerships and supports the protection of privacy and civil rights and civil liberties by enabling only the minimum necessary amount of personal information to be transferred in any particular transaction. Its implementation will be led by the Department of Commerce.

In September 2010, Secretary Napolitano and Secretary Gates co-signed a Memorandum of Agreement between DHS and DoD regarding cybersecurity. The MOA established a Joint Coordination Element (JCE) led by a DHS senior official at DoD's National Security Agency. The intent of the MOA was to enable DHS and DoD to leverage each other's capabilities, and more readily share cybersecurity information on significant cyber incidents. The JCE has been in place and building to fully operational capability since October 2010.

In December 2010, the DHS Science and Technology Directorate and NIST signed a Memorandum of Understanding with the Financial Services Sector Coordinating Council. The goal of the agreement is to speed the commercialization of cybersecurity research innovations that support our Nation's critical infrastructures. This agreement will accelerate the deployment of network test beds for specific use cases that strengthen the resiliency, security, integrity, and usability of financial services and other critical infrastructures.

COLLABORATIVE RISK MANAGEMENT FORUMS

The increased pace of collaborative cybersecurity operations between DHS and the private sector is due, in part, to standing public-private forums that support ongoing process improvements across the partnership. A few of these forums—the Cross-Sector Cyber Security Working Group, the IT CIKR Sector, and the Industrial Control Systems Joint Working Group—meet under the auspices of the Critical Infrastructure Partnership Advisory Council and conduct their activities consistent with the National Infrastructure Protection Plan (NIPP) partnership framework.

The Cross-Sector Cyber Security Working Group was established to address cross-sector cyber risk and explore interdependencies between and among various sectors. The working group serves as a forum to bring government and the private sector together to address common cybersecurity elements across the 18 CIKR sectors. They share information and provide input to key policy and planning documents including the NCIRP, the President's *Cyberspace Policy Review,* and the *National Strategy for Trusted Identities in Cyberspace.*

The IT CIKR Sector security partnership is comprised of DHS as the IT Sector Specific Agency, public sector partners in the IT Government Coordination Council, and private sector partners in the IT Sector Coordinating Council. This partnership forms to execute the IT Sector's risk management framework: To identify and prioritize risks to IT Sector critical functions, to develop and implement corresponding risk management strategies, and to report on progress of risk management activities and adjustments to the IT Sector's risk profile. IT Sector public-private partners worked collaboratively to produce the 2009 IT Sector Baseline Risk Assessment (ITSRA), prioritizing risks to the sector's critical functions, and have subsequently been working to finalize corresponding risk management strategies outlining a portfolio of sector risk management activities to reduce the evaluated risks from the ITSRA across the functions. Progress reporting on implementation of these risk management strategies will be provided in the IT Sector Annual Report (as required by the NIPP).

In partnership with the Department of Energy, which is the Sector Specific Agency responsible for the Energy Sector under the NIPP, the Industrial Control Systems Joint Working Group provides a vehicle for stakeholders to communicate and partner across all critical infrastructure sectors to better secure industrial control systems and manage risk. The Industrial Control Systems Joint Working Group is a representative group comprising owners and operators, international stakeholders, Government, academia, system integrators, and the vendor community. The purpose of the ICSJWG is to facilitate the collaboration of control systems stakeholders to accelerate the design, development, deployment, and secure operations of industrial control systems. Based on public and private sector partner input, CSSP uses the Industrial Control Systems Joint Working Group to inform its mission activities and deliver needed products and services.

As you are aware, cybersecurity training is essential to increasing awareness of threats and the ability to combat them. To that end, CSSP conducts multi-tiered training through web-based and instructor-led classes across the country. In addition, a week-long training course is conducted at CSSP's state-of-the-art advanced training facility at the Idaho National Laboratory to provide hands-on instruction and demonstration. This training course includes a red team/blue team exercise in which the blue team attempts to defend a functional mockup control system while the red team attempts to penetrate the network and disrupt operations. The positive response to this week-long course has been overwhelming, and the classes are filled within a few days of announcement. To date, more than 16,000 public and private sector professionals have participated in some form of CSSP training through classroom venues and web-based instruction.

CSSP also provides leadership and guidance on efforts related to the development of cybersecurity standards for industrial control systems. CSSP uses these industry standards in a variety of products and tools to achieve its mission.

First, CSSP uses and promotes the requirements of multiple Federal, commercial, and international standards in its Cyber Security Evaluation Tool (CSET), which has been requested by and distributed to hundreds of asset owners across each of the 18 CIKR sectors. Tool users are evaluated against these standards based on answers to a series of standard-specific questions. CSET is also used by CSSP assessment teams to train and bolster an asset owner's control system and cybersecurity posture in on-site assessments. In fiscal year 2010, the program conducted more than 50 on-site assessments in 15 different States and two U.S. territories, including several remote locations where the control systems represent potential single points of failure for the community. The program is planning for 75 on-site assessments in fiscal year 2011.

Second, CSSP developed the *Catalog of Control Systems Security: Recommendations for Standards Developers,* which brings together pertinent elements from the most comprehensive and current standards related to control systems. This tool is designed as a superset of control systems cybersecurity requirements and is available in the CSET and on the website for standards developers and asset owners.

Last, the CSSP provides resources, including time and expertise, to standards development organizations including NIST, the International Society of Automation, and the American Public Transportation Association. Experts provide content, participate in topic discussions, and review text being considered by the standards body.

THE GENERAL PUBLIC

While considerable activity is focused on public and private sector critical infrastructure protection, DHS is committed to developing innovative ways to enhance the general public's awareness about the importance of safeguarding America's computer systems and networks from attacks. Every October, DHS and its public and private sector partners promote efforts to educate citizens about guarding against cyber threats as part of National Cybersecurity Awareness Month. In March 2010, Secretary Napolitano launched the National Cybersecurity Awareness Challenge, which called on the general public and private sector companies to develop creative and innovative ways to enhance cybersecurity awareness. In July 2010, 7 of the more than 80 proposals were selected and recognized at a White House ceremony. The winning proposals helped inform the development of the National Cybersecurity Awareness Campaign, *Stop. Think. Connect.,* which DHS launched in conjunction with private sector partners during the October 2010 National Cybersecurity Awareness Month. *Stop. Think. Connect.,* has evolved into an on-going National public education campaign designed to increase public understanding of cyber threats and how individual citizens can develop safer cyber habits that will help make networks more secure. The campaign fulfills a key element of President Obama's *Cyberspace Policy Review,* which tasked DHS with developing a public awareness campaign to inform Americans about ways to use technology safely. The program is part of the NIST National Initiative for Cyber Education.

DHS is committed to safeguarding the public's privacy, civil rights, and civil liberties. Accordingly, the Department has implemented strong privacy and civil rights and civil liberties standards into all of its cybersecurity programs and initiatives from the outset. To support this, DHS established an Oversight and Compliance Officer within NPPD, and key cybersecurity personnel receive specific training on the protection of privacy and other civil liberties as they relate to computer network security activities. In an effort to increase transparency, DHS also publishes privacy impact assessments on its website, *www.dhs.gov,* for all of its cybersecurity systems.

CONCLUSION

Set within an environment characterized by a dangerous combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and a lack of comprehensive threat and vulnerability awareness, the cybersecurity mission is truly a National one requiring broad collaboration. DHS is committed to creating a safe, secure, and resilient cyber environment while promoting cybersecurity knowledge and innovation. We must continue to secure today's infrastructure as we prepare for tomorrow's challenges and opportunities. Cybersecurity is critical to ensure that Government, business, and the public can continue to use the information technology and communications infrastructure on which they depend.

DHS continues to engage, collaborate, and provide analysis, vulnerability, and mitigation assistance to its private sector CIKR partners. Our continued dedication to privacy and civil rights and civil liberties ensures a positive, sustainable model for cybersecurity engagement in the future. Finally, we work closely with our interagency partners in law enforcement, military, and intelligence, providing the full complement of Federal capabilities in preparation for, and in response to, significant cyber incidents.

Chairman Lungren, Vice Chairman Walberg, Ranking Member Clarke, and distinguished Members of the subcommittee, let me conclude by reiterating that I look forward to exploring opportunities to advance this mission in collaboration with the subcommittee and my colleagues in the public and private sectors. Thank you again for this opportunity to testify. I would be happy to answer your questions.

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

Now the Chairman recognizes Mr. Cauley to testify.

STATEMENT OF GERRY CAULEY, PRESIDENT AND CEO, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mr. CAULEY. Good morning, Chairman Lungren, Ranking Member Clarke, distinguished Members of the subcommittee, and fellow panelists. My name is Gerry Cauley. I am the President and CEO of the North American Electric Reliability Corporation, and I appreciate the opportunity to testify this morning.

NERC is an independent, nonprofit corporation, and our mission is to ensure the reliability of the bulk power system of North America, which includes both the United States and Canada. I wake up every day thinking of two words, “reliability” and “accountability.” We assure reliability of the bulk power system by working closely with industry to ensure that we are continuously learning and improving and striving for excellence and reliability of the bulk power system. We also ensure the accountability for a reliable system through our mandatory standards and our compliance program.

Some associate NERC as being an industry association. However, NERC has a very diverse mix of interests that we represent, including small and large customers, Government entities, and a diverse range of industry owners, operators, and users.

NERC was initially formed in 1968 and operated for several decades as a voluntary organization. In 2006, we were certified by the Federal Energy Regulatory Commission as the electric reliability organization within the United States, and we have similar authorities in Canada. In 2007, our standards became mandatory and enforceable for the power system, including nine cybersecurity standards that we have in effect.

In terms of the challenge for the grid, I think everyone recognizes that there is a lot of concern for the security of the power grid in North America, and we understand that the grid is essentially at the hub of all critical infrastructures and that everyone depends on a reliable supply of electricity. Over the past couple of decades, the power grid has become increasingly more digital as the grid was modernized to improve reliability and efficiency, cost and quality benefits.

What I want to assure you, though, despite becoming more digital, the underlying power grid is very robust and resilient. The underlying power grid is nondigital. It is not as weak as may be conveyed to some and certainly is not operated over the public internet.

Many companies have taken prudent steps, such as providing dedicated control networks, redundant systems, tight access controls, adopting best security practices and patches. Certainly every day business continuity, reliability, and security are at the foremost of the industry and the leadership, the CEO-level leadership of the industry.

That is not to say, however, that there are not vulnerabilities. There are very serious vulnerabilities and threats that we face, and there are very serious adversaries that would do harm to the power grid in North America. The challenge is that the network has become very interconnected, a series of very interconnected digital networks and communications, that we do have portals from our control systems to the internet and to business systems, and that our digital assets are very widely distributed. They are varied. They come from a range of suppliers, and some of those suppliers are international. So we do have challenges on the supply side as well.

What is NERC doing with regard to this? We have our standards, as I mentioned, and we are doing hundreds of audits across the industry to ensure that our standards are being followed. We are doing readiness reviews and sharing best practices. We are conducting an exercise in November of this year to test our National response capability.

We issue alerts in cooperation with Homeland Security and other agencies. We have issued alerts on Stuxnet, Aurora, BP, and tunneling in other areas. We are monitoring activities that might impact the grid.

I would like to turn finally to just the importance of the relationship to homeland security and the Federal Government. I think the key there is the sharing of actionable information that we can use to protect the grid, not sort of general and vague information but timely, operational-type information.

Homeland Security has helped us in terms of providing security clearances not only to NERC staff but to industry personnel and provides periodic briefings to help us better understand the threats and vulnerability. As Mr. McGurk mentioned, we are working on a memorandum of understanding to integrate our ES–ISAC, our Information Sharing Analysis Center with the National center that he is the head of.

In conclusion, NERC is working very closely with Homeland Security and other Government agencies to ensure our critical infrastructure. Every day I am focused on the reliability and security of the grid and the interests of the American public.

I am here to answer your questions, and I appreciate the opportunity to speak today. Thank you.

[The statement of Mr. Cauley follows:]

Prepared Statement of Gerry Cauley

April 15, 2011

introduction

Good morning Chairman Lungren, Members of the subcommittee and fellow panelists. My name is Gerry Cauley and I am the president and CEO of the North American Electric Reliability Corporation (NERC). I am a graduate of the U.S. Military Academy, a former officer in the U.S. Army Corps of Engineers, and have more than 30 years experience in the bulk power system industry, including service as a lead investigator of the August 2003 Northeast blackout and coordinator of the NERC Y2K program. I appreciate the opportunity to testify today on the topic "The DHS and the Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure."

NERC BACKGROUND

NERC's mission is to ensure the reliability of the bulk power system of North America and promote reliability excellence. NERC was founded in 1968 to develop voluntary standards for the owners and operators of the bulk power system (BPS).[1] NERC is an independent corporation whose membership includes large and small electricity consumers, Government representatives, municipalities, cooperatives, independent power producers, investor-owned utilities, independent transmission system operators and Federal power marketing agencies such as TVA and Bonneville Power Administration.

In 2007, NERC was designated the Electric Reliability Organization (ERO) by the Federal Energy Regulatory Commission (FERC) in accordance with Section 215 of the Federal Power Act (FPA), enacted by the Energy Policy Act of 2005. Upon approval by FERC, NERC's reliability standards became mandatory across the BPS. These mandatory reliability standards include Critical Infrastructure Protection (CIP) Standards 002 through 009, which address the security of cyber assets essential to the reliable operation of the electric grid. To date, these standards [and those promulgated by the Nuclear Regulatory Commission] are the only mandatory cybersecurity standards in place across the critical infrastructures of North America. Subject to FERC oversight, NERC and its Regional Entity partners enforce these standards, which are developed with substantial input from industry and approved by FERC, to accomplish our mission to ensure the reliability of the electric grid. In its position between industry and government, NERC embodies the often-invoked goal of creating effective partnerships between the public sector and the private sector.

As a result of society's growing dependence on electricity, the electric grid is one of the Nation's most critical infrastructures. The bulk power system in North America is one of the largest, most complex, and most robust systems ever created by man. It provides electricity to more than 334 million people, is capable of generating more than 830 gigawatts of power and sending it over 211,000 miles of high voltage transmission lines, and represents more than $1 trillion in assets. The electricity being used in this room right now is generated and transmitted in real time over a complex series of lines and stations from possibly as far away as Ontario or Tennessee. As complex as it is, few machines are as robust as the BPS. Decades of experience with hurricanes, ice storms, and other natural disasters, as well as mechanical breakdowns, vandalism and sabotage, have taught the electric industry how to build strong and reliable networks that generally withstand all but the worst natural and physical disasters while supporting affordable electric service. The knowledge that disturbances on the grid can impact operations thousands of miles away has influenced the electric industry culture of planning, operating, and protecting the BPS.

THE CYBERSECURITY CHALLENGE FOR THE GRID

Along with the rest of our economy, the electric industry has become increasingly dependent on digital technology to reduce costs, increase efficiency and maintain the reliability of the BPS. The networks and computer environments that make up this digital technology could be as vulnerable to malicious attacks and misuse as any other technology infrastructure. Much like the defense of this country, the defense of the BPS requires constant vigilance and expertise.

The assets that make up the BPS are varied and widespread. Consequently, the architecture within the systems varies from operator to operator. However, the computer systems that monitor and control BPS assets are based on relatively few elements of technology. Due to increasing efficiencies and globalization of vendors, the universe of suppliers for industrial control systems is limited. This trend is leading toward a fairly homogenous technological underpinning and, as older proprietary technology is replaced, the variation may decrease further.

For example, the bulk power system could be as vulnerable to digital threats as IT systems, but with far more critical implications. As proprietary industrial control systems continue to integrate Commercial Off-The-Shelf (COTS) systems, these plat-

[1] The Bulk Power System (BPS) is defined as generation and transmission of electricity greater than 100kv, in contrast to the distribution of electricity to homes and businesses at lower voltages.

forms could inherit the embedded vulnerabilities of those systems. As illustrated by the Stuxnet malware, industrial control system software can be changed and a loss of process control can occur without intrusions even being detected. The Stuxnet intrusion methods may serve as a blueprint for future attackers who wish to access controllers, safety systems, and protection devices to insert malicious code that could result in changes to set points and switches, as well as the alteration or suppression of measurements. NERC, through the Electricity Sector-Information Sharing and Analysis Center (ES–ISAC), issued an alert on Stuxnet, as it has done with other vulnerabilities, to inform the industry and recommend preventative action.

Establishment and continued refinement of NERC's enterprise risk-based programs, policies, and processes to prepare for, react to, and recover from cybersecurity vulnerabilities need to continue to be a high priority for the industry. The bulk power system has not yet experienced wide-spread debilitating cyber-attacks due in large part to the traditional physical separation between the industrial control system environment and business and administrative networks. However, the increased sharing of internet and computer networking by control systems and business and administrative networks means that digital infrastructures that were formerly physically separated are now becoming susceptible to common threats.

THE ROLE OF NERC AND CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS

The NERC CIP standards require electric sector entities to develop a risk-based security policy based upon their specific assets, architecture, and exposure. This policy, if properly implemented, will provide insight into the entity's systems and provide the opportunity to mitigate potential threats and vulnerabilities before they are exploited. Compliance with the NERC CIP standards is a first step in properly securing the BPS. However, there is no single security asset, security technique, security procedure, or security standard that, even if strictly followed or complied with, will protect an entity from all potential threats. The cybersecurity threat environment is constantly changing and our defenses must keep pace. Security best practices call for additional processes, procedures, and technologies beyond those required by the CIP standards. Simple implementation of enforceable standards, while valuable and a necessary first step should not be seen as the security end-state.

It is important to emphasize the difficulty of addressing grid security through a traditional regulatory model that relies principally on mandatory standards, regulations, and directives. The defensive security barriers mandated by CIP standards can be effective in frustrating ordinary hackers by increasing the costs and resources necessary to harm to the grid. They may not, however, stop the determined efforts of the intelligent, adaptable adversaries supported by nation states or more sophisticated terrorist organizations.

NERC is moving forward with a number of actions to complement our mandatory CIP standards and provide enhanced resilience for the grid. As chair of the Electricity Sub-Sector Coordinating Council (ESCC), I work with industry CEOs and our partners within the Government, including the Department of Energy, Department of Defense, and Department of Homeland Security, to discuss and identify critical infrastructure protection concepts, processes, and resources, as well as to facilitate information sharing about cyber vulnerabilities and threats. This type of public/private partnership is key to coordination and communication efforts on cybersecurity topics and initiatives. NERC is also developing a North American cybersecurity exercise to prepare for and test a National response plan for the electric sector.

The most effective approach for combating sophisticated adversaries is to apply resiliency principles, as outlined in a set of nine recommendations the National Infrastructure Advisory Council delivered to the White House in October 2010. I served on that Council, along with a number of nuclear and electric industry CEOs. Resiliency requires more proactive readiness for whatever may come our way. Resiliency includes providing an underlying robust system; the ability to respond in real-time to minimize consequences; the ability to restore essential services; and the ability to adapt and learn. The industry is already resilient in many aspects, based on system redundancy and the ability to respond to emergencies. To further enhance resiliency, examples of the NIAC team's recommendations include: (1) A National response plan that clarifies the roles and responsibilities between industry and Government; (2) improved information sharing by Government regarding actionable threats and vulnerabilities; (3) cost recovery for security investments driven by National policy or interests; and (4) a National strategy on spare equipment with long lead times, such as transformers. At NERC, we are working with stakeholders to develop programs that build upon the resiliency inherent in the grid to better secure critical assets and ensure the continued reliability of the BPS.

INFORMATION EXCHANGE IS CRITICAL

NERC and the electric industry can only deal with the risks they are aware of. It is impractical, inefficient, and impossible to defend against all possible threats or vulnerabilities. Entities must prioritize their resources to ensure that they are protected against those risks that pose the greatest harm to their assets, their business, and their customers. The electric industry is in the best position to understand the impact that a particular event or incident could have on the BPS, but they do not have the same access to actionable intelligence and analysis that the Government does. This lack of information leads the industry to be, at best, a step behind when it comes to protecting against potential threats and unknown vulnerabilities. Too often the industry has heard from Government agencies that the threats are real, but are given little or no additional information. This leads to frustration among the private sector leaders who are unable to respond effectively due to ill-defined and nebulous threat information.

NERC AND DHS

Improving the amount and quality of actionable intelligence available to industry is a priority for NERC and is reflected in a number of joint projects underway with DHS and DOD.

NERC is working with DHS' National Cybersecurity and Communications Integration Center to develop a Memorandum of Understanding for bi-directional sharing of critical infrastructure protection information between the Government and the electricity sector in North America. The MOU will result in cybersecurity data flow, analytical collaboration, and incident management activities across the spectrum of cybersecurity coordination to include detection, prevention, mitigation, and response/recovery.

NERC and DHS cooperative activities will align differing, but related missions, business interests, strengths, and capabilities to identify and develop mitigations for emerging cybersecurity risks, which will enhance the protection of critical infrastructure and Government networks and systems that are vital to National security and the Nation's economy. Under this MOU, NERC, as the ES–ISAC, will act as a clearing house, disseminating actionable intelligence, including classified contextual information to appropriately cleared staff within the BPS community. NERC also will provide anonymous situational awareness to DHS analysts to supplement the information DHS received from the intelligence community. We see this effort as crucial to improving the level of threat awareness within the industry and improving information between Government and industry.

As noted before, NERC also uses the ES–ISAC to send Alerts and Notifications to registered BPS entities. These Alerts and Notifications are developed with the strong partnership of Federal technical partners, including DHS and the Department of Energy National Laboratories, and BPS subject matter experts, called the HYDRA team by NERC.

NERC also provides leadership to two significant DHS-affiliated public-private partnerships. These are the Partnership for Critical Infrastructure Security (PCIS) and the Industrial Control Systems Joint Working Group (ICSJWG). The PCIS is the senior-most policy coordination group between public and private sector organizations. On the Government side, PCIS is comprised of the National Infrastructure Protection Plan (NIPP) Federal Senior Leadership Council (FSLC) and the State, Local, and Tribal Government Coordinating Council (SLTGCC), as well as the chairs of all of the other Government Sector Coordinating councils. On the private side, PCIS is comprised of the chairs of all of the private sector coordinating councils. The ICSJWG is a cross-sector industrial control systems working group that focuses on the areas of education, cross-sector strategic roadmap development, coordinated efforts on developing better vendor focus on security needs and cybersecurity policy issues.

NERC, DOE, AND DOD

NERC is engaged with other agencies besides DHS, including DOD and DOE National laboratories, to further the level of awareness and expertise focused on cybersecurity, especially as it pertains to the BPS. We are working with Pacific Northwest National Laboratory on developing certification guidelines for Smart Grid Cyber Operators and the Electric Sector Network Monitoring initiative. Similarly, we are working with the Idaho National Laboratory to promote the Cyber Security Evaluation Tool for use within the electric sector. NERC also is partnering with the Industrial Control Systems Cyber Emergency Response Team to share threat, vulnerability, and security incident information.

Additionally, NERC is working with DOE and the National Institute of Standards and Technology to develop comprehensive cybersecurity risk management process guidelines for the entire electric grid, including the BPS and distribution systems. We believe this to be particularly important with the increasing availability of smart grid technologies. While the majority of technology associated with the smart grid is found within the distribution system, vulnerabilities realized within the distribution system could potentially impact the BPS. Everyone engaged in smart grid implementation should ensure that appropriate security applications and technologies are built into the system to prevent the creation of additional threats and vulnerabilities.

CONCLUSION

As our Nation becomes more dependent upon electricity and as the BPS becomes more dependent on information systems, we must secure those systems that enable our way of life. As discussed today, NERC is committed to working with DHS and other Government agencies on several efforts to promote innovation and secure our critical infrastructure. As Congress considers policy decisions in this arena, NERC would suggest that the ESCC and the ES–ISAC be considered as key elements in the cybersecurity mission. NERC continues to work with Government and industry to utilize its expertise and promote thoughtful innovation as we address the question of how to ensure security in our open society. The cybersecurity challenges facing us are not intractable—they are the result of our own great innovation and can be overcome through our own great ingenuity.

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

Now the Chairman would recognize Ms. Carlin to testify.

STATEMENT OF JANE CARLIN, CHAIR, FINANCIAL SERVICES SECTOR COORDINATING COUNCIL

Ms. CARLIN. Thank you, Chairman Lungren and other Members of the committee, for hearing our thoughts today in this important area and for inviting me to testify on behalf of the Financial Services Sector Coordinating Council.

I am Jane Carlin, and I serve as chairperson of the council that we refer to as FSSCC. I have submitted a detailed written statement that addresses several areas, including how the FSSCC and others in the sector engage with DHS on cybersecurity issues, lessons learned from recent cyberattacks, recommendations for improved public-private information sharing, and comments on cybersecurity legislation. In the interest of time, I would like to focus mostly on information sharing today following a brief overview of the FSSCC.

FSSCC was created in 2002 in response to the September 11 attacks. It operates under the support of the U.S. Treasury as our sector-specific agency in harmony with a Presidential directive. The FSSCC does not collect dues. It is entirely a volunteer organization. Accordingly, it relies heavily on the time members contribute and to the expertise and leadership roles members play within their respective financial institutions and associations.

In recent years, FSSCC has had a highly productive and expanding relationship with DHS at the most senior levels and on many fronts, including information sharing, research and development, cyber exercises, and cross-sector coordination.

Information sharing is of critical importance to the financial services sector for several reasons. First, financial institutions and others that make up the critical infrastructure are on the front line of cybercrime and malicious attacks. When a financial institution is the victim of a cyberattack, it is concerned about protecting its customers, its reputation, and complying with all relevant regulatory requirements.

Second, others in the sector may be concerned about the impact that this attack could have on its organization and counterparties, as well, of course, as the potential for systemic risk to the entire financial services sector.

Third, the Government is responsible for enforcing laws and promoting critical infrastructure protection, and the Government ultimately holds important information that is both technical and contextual. Technical information such as malware signatures, contextual in terms of what type of entity appears to be initiating the attack.

There is a strong need to establish appropriate and well-understood protocols to share information so that we collectively understand the problems and risks that we face in order to arrive at the right response or solution. When attacks occur, the FSSCC has a defined crisis management process, escalation and notification protocols, including sending rapid notifications to members throughout financial services.

Although we have made good progress in creating information-sharing entities and mechanisms for information sharing, we have not adequately tackled the critically important issues associated with timeliness and completeness of information sharing. We now need to focus on clarifying and compartmentalizing information so that so-called actionable intelligence can be disseminated to responsible parties that will use it to protect critical infrastructure.

What I mean by actionable intelligence is simply redacted technical and contextual information without revealing sources and uses or tipping off criminals or adversaries.

The fundamental issue of striking a balance between confidentiality for criminal investigations and timely information sharing remains a work in progress. An example of an incident where too much secrecy led to an increased exposure was the cyberattacks on a major exchange which was discovered by the exchange in October, 2010. The exchange alerted its primary regulator in law enforcement for a variety of reasons, including an investigation of the attack by law enforcement and intelligence agencies. Information about the attack and its impact on other financial institutions was not disclosed to others in the financial services sector for 102 days. The lack of meaningful information sharing for more than 3 months left the entire sector unnecessarily vulnerable.

In this connection, we would like to suggest two recommendations: First, a more transparent decision-making process to facilitate information sharing would accelerate the dissemination of information without interfering or undermining criminal or National security investigations. To implement this kind of information-sharing protocol, the FSSCC and senior DHS officials have agreed in principle to collaborate on protocols for sharing technical and contextual information, again without interfering with an on-going investigation.

Second, we believe that DHS needs to regularly leverage the security clearances that DHS and other Government agencies have sponsored for members of the FSSCC as part of the information-sharing framework. The Government should be able to more easily consult with industry experts and to better understand the systemic risk implications of these cyber events by leveraging the secured and cleared community.

On behalf of the FSSCC, I ask this committee in its oversight capacity to support DHS's work in these areas. It is my hope that this good work to enhance the public-private partnership will continue so that together we can be more resilient and combat those who would seek to undermine our economy and stability, be they homegrown or foreign, criminal or terrorist, rogue- or State-sponsored. It is only by working together that we will prevail in the complex and ever-changing internet-connected world.

Thank you.

[The statement of Ms. Carlin follows:]

Prepared Statement of Jane Carlin

April 15, 2011

Chairman King, Subcommittee Chairman Lungren, Ranking Member Thompson and Members of the subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Homeland Security Committee, I am Jane Carlin. I serve as the chairperson of Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security ("FSSCC"). I also am the Managing Director and Global Head of Operational Risk, Business Continuity, Information Security, and Risk and Insurance Management at Morgan Stanley.

Thank you for inviting me to testify on behalf of the Financial Services Sector Coordinating Council for Homeland Security and Critical Infrastructure Protection ("FSSCC") on "The Department of Homeland Security Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure." My testimony today will address the following: Background information on the FSSCC, engagement with DHS, lessons learned from recent cyber attacks, recommendations for improving public-private partnership, and comments on cybersecurity legislation.

BACKGROUND ON FSSCC AND PUBLIC-PRIVATE PARTNERSHIP

The FSSCC was established in 2002 in response to the September 11, 2001 attacks and at the request of the U.S. Treasury Department in harmony with Presidential Decision Directive 63 of 1998. Presidential Decision Directive 63 required sector-specific Federal departments and agencies to identify, prioritize, and protect United States critical infrastructure and key resources and to establish partnerships with the private sector.

The FSSCC has 52 member associations and financial institutions representing clearinghouses, commercial banks, credit rating agencies, exchanges/electronic communication networks, financial advisory services, insurance companies, financial utilities, Government-sponsored enterprises, investment banks, merchants, retail banks, and electronic payment firms.[1] FSSCC members dedicate a significant amount of time and resources to this partnership for critical infrastructure protection and homeland security. The FSSCC does not collect dues and its success as a volunteer organization relies heavily on the time members contribute and to the expertise and leadership roles members play within their respective financial institutions and associations. Appendix A includes the current FSSCC organizational chart, including those who serve in leadership roles of seven committees that ad-

[1] Members including: American Bankers Association, American Council of Life Insurers, American Insurance Association, American Society for Industrial Security International, BAI, Bank of America, Bank of NY/Mellon, Barclays, BITS/The Financial Services Roundtable, CME Group, ChicagoFIRST, Citigroup, The Clearing House, CLS Group, Consumer Bankers Association, Credit Union National Association, The Depository Trust & Clearing Corporation, Fannie Mae, Financial Industry Regulatory Authority, Financial Information Forum, Financial Services Information Sharing and Analysis Center, Freddie Mac, Futures Industry Association, Goldman Sachs, ICE Futures U.S., Independent Community Bankers of America, Investment Company Institute, JP Morgan Chase, Managed Funds Association, Morgan Stanley, NACHA—The Electronic Payments Association, The NASDAQ Stock Market, Inc., National Armored Car Association, National Association of Federal Credit Unions, National Futures Association, Navy Federal Credit Union, NYSE Euronext, The Options Clearing Corporation, Securities Industry and Financial Markets Association, State Farm, State Street Global Advisors, Travelers, VISA USA Inc.

dress crisis event management, cross-sector coordination, cybersecurity, international, long-range vision, policy, and research and development.

On August 3, 2010, I was selected by members of the FSSCC to serve as the chairperson. I am preceded by four FSSCC chairpersons: Shawn Johnson of State Street Global Advisors (SSGA) from 2008–10, George Hender of the Options Clearing Corporation (OCC) from 2006–08, Don Donahue of Depository Trust and Clearing Corporation (DTCC) from 2004–06, and Rhonda MacLean of Bank of America from 2002–04. Prior to my selection, I served as FSSCC's vice chairperson and head of the FSSCC Cybersecurity Committee from June 2008 to August 2010. Additionally, I serve on the Executive Committee and Board of the Partnership for Critical Infrastructure Security (PCIS), which is the private sector organization that coordinates homeland security issues for all National critical infrastructure sectors.

Each year the FSSCC submits an annual report on our activities. This annual report is published by the Department of Homeland Security along with reports from the other CIP sectors. Appendix B is the executive summary of our most recent Sector Annual Report which provides an overview of our role and activities. Our partnership is frequently heralded as the model and aspired to by the other 17 critical infrastructure sectors.

The goal of the FSSCC is to continue to improve the resilience and availability of financial services by working through its public-private partnership to address the evolving nature of threats and vulnerabilities and the risks posed by the sector's dependence on other critical sectors. In support of this goal, the FSSCC established four objectives in 2010:

- Identify threats and promote protection;
- Drive preparedness;
- Collaborate with the Federal Government;
- Coordinate crisis response.

In support of these objectives the FSSCC's current priorities include:

- Information sharing;
- Crisis event management;
- Threat matrix dissemination and management;
- Communication and outreach;
- Identity assurance.

In 2002, the Treasury Department also chartered the Financial and Banking Information Infrastructure Committee (FBIIC) under the President's Working Group on Financial Markets.[2] The FBIIC is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting the public/private partnership. The U.S. Department of the Treasury serves as the Sector Specific Agency (SSA) for the Banking and Finance Sector. The FSSCC–FBIIC public-private partnership was confirmed in Homeland Security Presidential Directive 7 of 2003.

The FSSCC and FBIIC meet jointly at least three times a year, supplemented by monthly conference calls. Earlier this week, over 80 executives, experts, and officials from the FSSCC and FBIIC met in Chicago to discuss a wide range of issues, including: Information sharing, regional coalitions, threats, and cyber incident reviews.

In addition to the collaboration with the FBIIC, it is important to remind the committee that the financial services sector is highly regulated by international, Federal, and State authorities. Through numerous laws enacted by Congress over the past 150 years, Federal financial regulators have implemented a complex regime that includes supervision of the financial institutions' operational, financial, and technological systems. Regulators, such as the Federal Reserve, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency and Securities and Exchange Commission, conduct examinations to assess the adequacy of controls to address financial and other risks. These examinations focus on information security, business continuity, vendor management, and other operational risks.

In addition to these public sector entities, self-regulatory organizations (SROs), such as the Municipal Securities Rulemaking Board (MSRB), the Financial Industry Regulatory Authority (FINRA), the National Futures Association (NFA), and ex-

[2] The FBIIC was organized under Executive Order 13231 of October 16, 2001 entitled *Critical Infrastructure Protection in the Information Age.* Members of the FBIIC include: American Council of State Savings Supervisors; Commodity Futures Trading Commission; Conference of State Bank Supervisors; Department of the Treasury; Farm Credit Administration; Federal Deposit Insurance Corporation; Federal Housing Finance Agency; Federal Reserve Bank of New York; Federal Reserve Board; National Association of Insurance Commissioners; National Association of State Credit Union Supervisors; National Credit Union Administration; North American Securities Administrators Association; Office of the Comptroller of the Currency; Office of Thrift Supervision; Securities and Exchange Commission; and Securities Investor Protection Corporation.

changes, such as the Chicago Mercantile Exchange (CME), and the New York Stock Exchange (NYSE), also play an important role in industry oversight.

ENGAGEMENT WITH DHS

The FSSCC has a productive and expanding relationship with the Department of Homeland Security (DHS), but more is needed. Our engagement with DHS covers a wide range of activities, including crisis management, information sharing, research and development, and managing the risks posed by our sector's dependency on other critical sectors, such as communications and information technology, for which DHS serves as the SSA. In addition to meeting with senior officials at DHS, the FSSCC and FS–ISAC have engaged in numerous projects and initiatives to improve critical infrastructure and cybersecurity, including:

Information Sharing and Threat Identification.—On a daily basis, there are cyber attacks. The financial services sector develops its own information about threats, vulnerabilities, and incidents. These threats, vulnerabilities, and incidences are shared within the protection protocols of the sector. Financial institutions view the risk environment much broader than just within our individual organizations. Given the interconnections and risk exposure among participants and counterparties, an attack on one institution could have cascading implications for others in the sector.

When cyber attacks occur, the FSSCC has a defined crisis management process, escalation and notification protocols to share information. As part of this process, our sister organization, the Financial Services Information Sharing and Analysis Center (known as the "FS–ISAC"), sends rapid notifications to member firms to protect critical systems and assets.

The FS–ISAC reaches more than 20,000 sector participants daily and promotes information sharing between the public and private sectors. The FS–ISAC allows its members to receive threat and vulnerability information immediately; communicate within a secure portal to share vulnerability assessments and other information anonymously; and access new data feeds of threat and vulnerability information. In addition, the FS–ISAC has implemented a crisis communications system to notify its members of emergencies in minutes.

In 2010, the Financial Services Information Sharing and Analysis Center (FS–ISAC), which serves as the information-sharing operational arm of the FSSCC, the Department of Defense and DHS, collaborated to launch the Government Information Sharing Framework initiative (GISF) based on initiatives with the Defense Industrial Base (DIB). This pilot program consists of information sharing of threat and attack data between the Federal Government and about a dozen financial services firms. Beyond this, the FS–ISAC is the third sector (following the Communications and IT sectors) to embed at the classified level, senior and operational representatives within the DHS National Cybersecurity and Communications Integration Center (NCCIC) as core members of the watch and response teams. The Government's plan is to use these examples as models for public-private sector information sharing for other sectors to follow.

In early April, senior DHS officials and the FSSCC agreed to collaborate on developing guidelines for when information should be shared, especially information that is technical and contextual. This decision to collaborate arose in response to a review of lessons learned from recent cyber attacks, which I will review in greater detail later in my testimony. In addition, the FSSCC is working with the National Infrastructure Assurance Council (NIAC) on an information-sharing study.

Sponsoring Security Clearances for Industry Professionals.—At the urging of the FSSCC years ago, DHS and the Treasury have increased the number of clearances for senior executives and experts from our sector. In addition, DHS and the Treasury have arranged classified level briefings each year, typically in conjunction with the FSSCC and FBIIC meetings. Dozens of FSSCC members and all member firms represented on the FS–ISAC Threat Intelligence Committee (TIC) are cleared to at least the SECRET level. In addition, at least seven financial services private sector individuals with cybersecurity responsibilities are cleared at TOP SECRET/SCI level. For those individuals who have been cleared, the process took a significant amount of time (not to mention the time and expense from the Government side).

Collaborate on R&D.—The FSSCC R&D Committee has been working closely with the Science and Technology Directorate of DHS for many years. Our collaboration began in 2005 when the FSSCC established an R&D Committee and shared the results of our efforts to identify the top R&D priorities.[3] Recently, we have focused

[3] See *https://www.fsscc.org/fsscc/news/default.jsp* for the list of top R&D priorities including: Advancing the state of the art in designing and testing secure applications; making financial transaction systems more secure and resilient; improving enrollment and identity credential

considerable attention on improving identity assurance. Our collaboration resulted in a groundbreaking Memorandum of Understanding (MOU), which was signed on December 6, 2010 by the FSSCC, DHS, and the National Institute of Standards and Technology (NIST) with active support by the White House Cybersecurity Advisor and head of the Office of Science and Technology Policy.[4] The MOU lays the foundation for developing an identity assurance test bed that will focus on improving the accuracy and timeliness of identity proofing, and reducing identity impersonation. The collaborative initiative includes the concept of a "financial services credential verification gateway" to enable direct verification of identity credentials with the authenticating authorities.

As a follow-up to the MOU, the FSSCC is working with DHS and NIST on a Cooperative Research and Development Agreement (CRADA) on identity proofing. Also envisioned in the MOU is an effort to define and test the concept of establishing a secure domain within the larger internet, where critical industries and Government can more securely exchange sensitive information and complete high-risk transactions. This effort also includes planning and testing for IPv6 and DNSSEC transitioning.

Other R&D activities include establishing and/or expanding relationships with academia, DHS, National Science Foundation (NSF), NIST, and the Department of Defense's Networking and Information Technology Research and Development (NITRD) to provide financial services expertise and enhance the transfer of promising research into commercial use. In addition, members of the FSSCC have participated in an insider threat study that DHS's U.S. Secret Service has been conducting for several years.

Comments on Strategies and Cyber Incident Response Plans.—The FSSCC has worked with DHS and White House officials in commenting on the National Strategy for Trusted Identities in Cyberspace (NSTIC). The FSSCC also has provided input into the National Cyber Incident Response Plan and supported the National Security Telecommunications Advisory Committee (NSTAC) Cross Sector Information Sharing Pilot.

Cross-Sector Coordination.—The FSSCC continues to work with cross-sector councils. For example, the FSSCC and FS–ISAC participate in the DHS Cross Sector Cyber Security Working Group (CSCWG), which has representation across the 18 critical infrastructure sectors and meets monthly to review cross-sector cybersecurity strategies, programs, and projects of interest. From a crisis management perspective, the FS–ISAC presence in both the National Infrastructure Coordination Center (NICC) and the NCCIC supports close cooperation and coordination for disaster, physical security, and cybersecurity events. We also are working with the other critical sectors through the Partnership for Critical Infrastructure Security (PCIS), an "arm" of DHS's partnership structure outlined in the NIPP, to share critical contact information for each sector as a first step to developing an efficient all hazards cross-sector crisis response plan.

In 2010, a more formal cross-sector information-sharing pilot was funded by the President's National Security Telecommunications Advisory Committee (NSTAC). Four sectors participated in this pilot: Financial services, communications, IT, and the defense industrial base. The FS–ISAC provided the secure portal by which the four sectors exchanged cyber threat data. Relevant and actionable cyber threat information was exchanged during the pilot, which would not have been known to the other sectors. As a result of the program's success, the pilot was extended in 2011 with the intent of rolling it out to all interested sectors later in the year. Furthermore, the FSSCC is involved in cross-sector work of the PCIS in order to share critical contact information for each sector as a first step to developing an efficient cross-sector crisis response plan.

Participation in Cyber Exercises and Crisis Playbooks.—The financial services sector has performed multiple exercises testing various perceived vulnerabilities and establishing follow-up actions as a result of lessons learned. Significant tests were run to evaluate sector preparedness related to social engineering attacks, payment processing attacks, and communication during a crisis. In particular, the 2009 Cyber Financial Industry and Regulators Exercise (CyberFIRE) and Cyber Attack against Payment Processes (CAPP) exercise were jointly executed by the FSSCC, FS–ISAC, and included many FBIIC members, the U.S. Secret Service, the Federal Bureau of Investigation (FBI), DHS, and more than 800 individual participants. Members of

management; understanding human insider threats and developing deterrence and detection; developing data-centric protection strategies to better classify and protect sensitive information; devising better measures of the value of security investments; and developing practical standards to reduce risk and enhance resiliency.

[4] See *http://www.whitehouse.gov/blog/2010/12/06/partnership-cybersecurity-innovation.*

the FSSCC are also planning to participate in the upcoming National Level Exercise No. 13 in May. The FSSCC and FS–ISAC have created crisis response playbooks in order to clarify lines of communication during crises. The sector provided leadership for recent events requiring a coordinated response, including the earthquake in Haiti, pandemic flu, and hurricane situations.

Support for Regional Coalitions and Fusion Centers.—Since 2002, the FBIIC and the FSSCC have supported the formation of regionally-based financial partnerships and coalitions dedicated to enhancing the resilience of the financial community in specific geographic areas. At present, there are nearly two dozen regional coalitions that consist of private sector members who partner with the public sector. DHS and the Treasury Department have been very supportive of these organizations, primarily through the Regional Partnership Council (RPC*first*), the umbrella organization to which the coalitions belong. Chicago FIRST, as the Chair of RPC*first*, partnered with the DHS National Cyber Security Division (NCSD) to develop "cyber tabletop in a box." Regional coalitions are conducting these tabletop exercises involving Federal, State, and local law enforcement in their respective regions. In addition, there are 72 fusion centers where experts from various Federal and local government agencies share information and collaborate with private sector participants.

Supply Chain Risks.—One of the emerging issues that FSSCC members are evaluating is the security of the global supply chain. Members continue to seek better assurances from our vendors that the major information technology and communications hardware and software systems that we deploy in our networks employ secure development practices and are free from malware or other threats that may have been implanted in the supply chain process. For example, in 2010, the sector published, the *Resilient International Telecommunications Guidelines for the Financial Services Sector,* highlighting the international risks associated with the undersea cables network.[5] This report identified both the risks associated with a critical infrastructure component, provided guidelines for managing those risks, and the need for increased international collaboration. The FSSCC worked closely with FBIIC members, most notably the Federal Reserve Board, and the National Communications System, a division of DHS, that works closely with major telecommunications providers.

INFORMATION SHARING LESSONS LEARNED FROM RECENT CYBER ATTACKS

Information sharing is of critical importance to the financial services sector, other critical infrastructure sectors and the Government. Without it, none of the FSSCC's other top priorities—crisis event management, threat matrix dissemination and management, identity assurance—would be achievable. Although we have made good progress in creating information-sharing entities, to share information securely and efficiently, we have not adequately tackled the critically important issues associated with the timeliness and completeness of information. We now need to focus on clarifying and compartmentalizing information so that "actionable intelligence" can be disseminated to responsible parties that will use it to protect critical infrastructure. What I mean by "actionable intelligence" is redacted technical information and contextual information without revealing sources and uses or tipping off criminals or adversaries.

Information sharing among financial institutions, other critical infrastructure sectors, and the Government is important for several reasons. First, a company that is a victim of a cyber attack is concerned about protecting its customers, its reputation and complying with regulatory requirements. Second, others in the sector are concerned about the impact that this a cyber attack could have on its organization and counterparties or provider might have on their operations, as well as the potential for systemic risk to entire financial services sector. Third, the Government is responsible for enforcing laws and promoting protecting critical infrastructure protection. The Government also holds important information that is both technical, such as malware signatures, and contextual, such as what type of entity appears to be initiating the attack. This is due to the Government's own operations in cyberspace and other roles including law enforcement, defense, and regulation.

There is a strong need to establish appropriate and well-understood protocols to share information so that we collectively understand the problems and risks that we face in order to arrive at the right response or solution. The fundamental issue of striking a balance between confidentiality for criminal investigations and timely information sharing remains a work in progress.

An example of an incident where too much secrecy led to an increased exposure was the cyber attack on a major exchange, which was discovered by the exchange

[5] See *https://www.fsscc.org/fsscc/publications/default.jsp.*

in October 2010. The exchange alerted its primary regulator and law enforcement. For a variety of reasons, including an investigation of the attack by law enforcement and intelligence agencies, information about the attack and its impact on other financial institutions was not disclosed to others in the financial services sector for 102 days. This 102-day period included year-end, when financial institutions closed their books and prepare annual reports. This could have had an enormous impact on employees, stockholders, large and small, and the market as a whole. The lack of meaningful information for more than 3 months left the entire sector unnecessarily vulnerable.

In response to this event and recent discussions with senior DHS officials, the FSSCC and DHS have agreed to collaborate on developing guidelines for when information should be shared, especially information that is technical and contextual. FSSCC members believe that a more transparent decision-making process would accelerate the dissemination of information without interfering or undermining criminal and National security investigations. We also hope that these protocols will elevate the priority that government places on sharing information associated with protecting critical infrastructure. Also, by leveraging the security clearances that DHS and other Government agencies have sponsored for members of the FSSCC, the Government could consult with industry experts to better understand the systemic risk implications of the cyber events.

RECOMMENDATIONS FOR IMPROVING PUBLIC-PRIVATE PARTNERSHIP

FSSCC recommends the following activities to improve the public-private partnership with DHS and other Government agencies:

1. Protecting Critical Infrastructure Through Enhanced Information Sharing.—We have made good progress in creating utilities to share information securely and efficiently. However, we have not adequately tackled the critically important issues associated with the timeliness and completeness of information. We now need to focus on clarifying and compartmentalizing information so that it can be disseminated via the FS–ISAC. This is also important for the Government to better understand the significance of information, including the impact on the critical infrastructure sectors. We cannot assume the Government will know how to evaluate the risks unless experts from the financial services sector (or other CIP sectors) have a seat at the table. We also recognize that there will be times when the Government cannot consult with industry sectors and thus there needs to be clarity as to when and how information will be shared.

As noted earlier in my testimony, FSSCC and DHS have agreed to collaborate on developing guidelines for when information should be shared, especially information that is technical and contextual. Together, we need to learn from the recent breaches and establish guidelines where we have more predictability in knowing when information will be shared.

Building trust and enhancing understanding is a compelling reason for expanding the number of clearances to senior executives and experts in the financial services sector who are in position to "operationalize" timely and relevant threat and attack intelligence. We also urge DHS to establish clearer protocols for the sponsorship of private sector security clearances that are not directly related to a Government contract and for non-U.S. citizens. We recognize that this is a fairly new development and one which does not have clear protocols, either among the sponsoring agencies, or in the private sector. A system that would identify and categorize critical job functions into "need to know" status should effectively expand the community of private sector stakeholders who can get early Government notification of significant issues. FSSCC members also suggest better "tearline" documents and the availability of classified information on a geographically, disaggregated basis. Moreover, nationality is a consideration not covered under current "cold war"-derived clearance protocols as not all the appropriate individual's in corporate information security group who have a "need-to-know" homeland cybersecurity information are U.S. citizens. We propose that the clearance mechanism should expand to consider at minimum clearing individuals from the UKUSA agreement countries (United Kingdom, Canada, Australia, and New Zealand) and other countries, as possible, based on government-to-government background check arrangements.

We need to enhance improve information sharing with the communications, information technology, and electricity sectors. Currently the FS–ISAC and FSSCC have little to no operational transparency into other sectors. This may somewhat be addressed by the embedding of personnel in the NCCIC however further policy and engagement is required to provide a Common Operating Picture (COP) across those dependent infrastructures.

2. *Conduct more exercises and training.*—In addition to clearances and information sharing, we have found that we build greater trust through exercises and training. By routinely engaging in exercises and training through tabletop exercise, meetings, and awareness campaigns we bring the right public and private sector participants together on a regular basis. Working together, building relationships and establishing trust are essential parts of creating a culture that can share useful and timely information. The embedding of financial sector personnel in the NCCIC and NICC is a positive step in that engagement process.

3. *Invest in R&D.*—In addition to supporting the MOU and CRADAs on identity assurance, we also encourage the Government to look to emerging research on automated methods of attack detection, communication, and prevention. As an example of the possibilities that could be considered, DHS released a white paper entitled, *Enabling Distributed Security in Cyberspace.* While this was only a concept paper, it suggests a thoughtful, if ambitious vision for the future where: “A healthy cyber ecosystem would interoperate broadly, collaborate effectively in a distributed environment, respond with agility, and recover rapidly. With a rich web of security partnerships, shared strategies, preapproved and prepositioned digital policies, interoperable information exchanges, . . . healthy cyber ecosystem could defend against a full spectrum of known and emerging threats, including attacks against the supply chain, remote network-based attacks, proximate or physical attacks, and insider attacks . . .”.[6]

4. *Coordinate efforts internationally.*—Cybersecurity is not an issue that can be defined by geographic or political borders. The National Cybersecurity and Communications Integration Center is slowly making strides in bringing together industry and Government operational capabilities under one roof, breathing the same air, to create a cross-sector common operational picture about our cyber threats and vulnerabilities. The FS–ISAC has a seat in the NCCIC, and both FSSCC and FS–ISAC are participating in the Unified Coordination Group that is developing the NCCIC’s information sharing and incident response process.

The FSSCC recognizes that this is a difficult endeavor—one that involves numerous complexities around National security intelligence, legal authorities, regulatory requirements, privacy protections, and contractual restrictions. We are not where we need to be yet, but we are moving in the right direction—to an envisioned end state where private sector members of the NCCIC are able to communicate threat intelligence in real time to their sector partners and coordinate protective or mitigating action jointly with the Government and other sectors.

COMMENTS ON CYBERSECURITY LEGISLATION

The committee had also asked for me to comment on cybersecurity legislation. In general, the FSSCC is supportive of policies in which a “rising tide lifts all boats”. By that I mean the Government should offer incentives and, in some cases, require minimum security and resiliency standards for utilities that service critical infrastructure sectors. These utilities include entities like internet service providers and others with whom our sector and other critical infrastructure sector are dependent. For example, we need to ensure that these utilities adopt practices to protect networks, manage incidences, and address our long-standing concerns with internet congestion during a time of crisis.[7] The development of these standards should be driven by private sector, consensus-driven bodies. What has been lacking is a comprehensive cross-cutting review of the cyber risk, mitigation, and regulatory dynamics across all of the critical sectors to ensure that any “minimum standards” legislation can allow specific security gaps in each sector to be addressed without imposing one-size-fits-all standards that contradict existing sector regulation.

The FSSCC supports the following provisions:

- Commitment to two-way public-private information sharing and cross-sector information-sharing efforts, leveraging the Information Sharing and Analysis Centers (ISACs), the Sector Specific Agencies (SSAs), US–CERT, safe harbors, clearances, and confidentiality guarantees. Such a commitment is vital to facilitate the sharing of actionable and timely information, particularly during cyber emergencies.

[6] *http://www.dhs.gov/xlibrary/assets/nppd-healthy-cyber-ecosystem.pdf.*

[7] U.S. Department of Homeland Security, *Pandemic Influenza Impact on Communications Networks Study,* December 2007. *http://www.ncs.gov/library/pubs/Pandemic%20Comms%20Impact%20Study%20%20Best%20Practices.pdf;* GAO, *Influenza Pandemic: Key Securities Market Participants Are Making Progress, but Agencies Could Do More to Address Potential Internet Congestion and Encourage Readiness,* GAO–10–8, October 2009. *http://www.gao.gov/new.items/d108.pdf.*

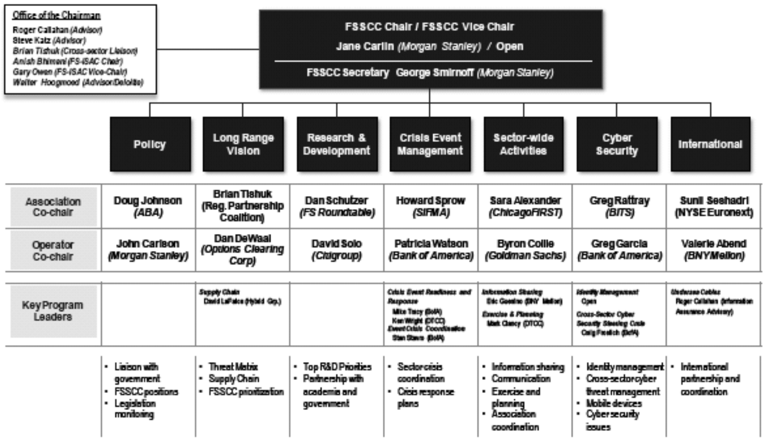
- Focused efforts to address critical interdependencies such as our sector's reliance on telecommunications, information technology, energy, and transportation sectors.
- Leveraging Federal cybersecurity supply chain management and promotion of cybersecurity as a priority in Federal procurement.
- Public education and cybersecurity awareness campaigns to promote safe computing practices.
- Enhanced international collaboration and accountability in law enforcement and industry, including increased funding for law enforcement and facilitating the development of global cybersecurity standards.
- Increasing funding for applied research and encouraging collaboration with Government research agencies on authentication, access control, identity management, attribution, social engineering, data-centric solutions, and other cybersecurity issues. It is only through such public-private efforts, combined with adequate funding, that leading-edge research in these important areas can enhance our ability to secure on-line transactions, maintain data integrity, and enhance user confidence.
- Attention to ICANN and other international internet governance bodies especially as ICANN begins a new application round for what could be as many as a thousand new top-level internet domains later this year. It is vitally important that effective oversight exist to enhance security and privacy protections.
- Need for enhanced supervision of service providers on whom financial institutions depend, while at the same time recognizing the role of Federal financial regulators in issuing regulations and supervisory guidance on security, privacy protection, business continuity, and vendor management for financial institutions and for many of the largest service providers. Strengthening Government-issued credentials (e.g., birth certificates, driver's licenses and passports) that serve as foundation documents for private sector identity management systems.

The FSSCC does not support provisions that provide sweeping new authority for the Executive branch to remove access to the internet and other telecommunications networks, without clarifying how, when, and to what extent this would be applied to our critical infrastructures. Such a provision also sets the wrong precedent in light of recent restrictions on internet use imposed in other countries.

CONCLUSION

In conclusion, I would like to thank the committee for inviting me to testify today on behalf of the FSSCC on the DHS cybersecurity mission and how they interact with private sector owners. Both the public and private sector financial services organizations recognize the importance of improving information sharing as part of continuity planning, crisis management, and enhancing resiliency in preparing for and responding to significant events. We know that during a real crisis we cannot operate as independent entities and thus we must establish trusted relationships and plan ahead of time so that we are prepared to respond to a real crisis. It is my hope that the good work done to date in bridging the public-private divide by FSSCC and DHS continues and that we find additional ways to effectively combat those who would seek to undermine our economy and stability—be they homegrown or foreign, criminal or terrorist, rogue or state-sponsored. It is only by working together that we will prevail in the complex and every changing internet-connected world.

Appendix A: FSSCC Org Chart



Office of the Chairman
Roger Callahan *(Advisor)*
Steve Katz *(Advisor)*
Brian Tishuk (Cross-sector Liaison)
Anish Bhimani (FS-ISAC Chair)
Gary Owen (FS-ISAC Vice-Chair)
Walter Hoogmoed (Advisor/Deloitte)

FSSCC Chair / FSSCC Vice Chair
Jane Carlin *(Morgan Stanley)* / Open
FSSCC Secretary George Smirnoff *(Morgan Stanley)*

	Policy	Long Range Vision	Research & Development	Crisis Event Management	Sector-wide Activities	Cyber Security	International
Association Co-chair	Doug Johnson *(ABA)*	Brian Tishuk (Reg. Partnership Coalition)	Dan Schutzer *(FS Roundtable)*	Howard Sprow *(SIFMA)*	Sara Alexander *(ChicagoFIRST)*	Greg Rattray *(BITS)*	Sunil Seshadri (NYSE Euronext)
Operator Co-chair	John Carlson *(Morgan Stanley)*	Dan DeWaal *(Options Clearing Corp)*	David Solo *(Citigroup)*	Patricia Watson *(Bank of America)*	Byron Collie *(Goldman Sachs)*	Greg Garcia *(Bank of America)*	Valerie Abend *(BNYMellon)*
Key Program Leaders		*Supply Chain* David LaFalce (Hybrid Grp.)		*Crisis Event Readiness and Response* Mike Tracy (BoA) Ken Wright (DTCC) *Event Crisis Coordination* Stan Stearns (BoA)	*Information Sharing* Eric Guerrino (BNY Mellon) *Exercise & Planning* Mark Clancy (DTCC)	*Identity Management* Open *Cross-Sector Cyber Security Steering Cmte* Craig Froelich (BofA)	*Undersea Cables* Roger Callahan (Information Assurance Advisory)
	• Liaison with government • FSSCC positions • Legislation monitoring	• Threat Matrix • Supply Chain • FSSCC prioritization	• Top R&D Priorities • Partnership with academia and government	• Sector crisis coordination • Crisis response plans	• Information sharing • Communication • Exercise and planning • Association coordination	• Identity management • Cross-sector cyber threat management • Mobile devices • Cyber security issues	• International partnership and coordination

Appendix B: Executive Summary of Sector Annual Report

executive summary

In 2003, the Banking and Finance Sector, hereinafter referred to as the Financial Services Sector, was identified as a critical infrastructure sector pursuant to Homeland Security Presidential Directive 7 (HSPD–7); the U.S. Department of the Treasury was identified as the Sector-Specific Agency (SSA) for the sector. As the SSA, the Treasury Department works with its public and private sector partners to maintain a robust sector that is resilient against manmade or natural incidents. The Financial Services Sector is essential to the efficiency of world economic activity. This Sector Annual Report outlines the requirements for current and future protective programs based on HSPD–7.

Both the private and public sectors, through the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) and the Financial and Banking Information Infrastructure Committee (FBIIC), respectively, have key roles in implementing the Financial Services Sector's critical infrastructure and key resources (CIKR) protective programs. Through direct mandates and regulatory authority, Federal and State financial regulators have specific regulatory tools that they can implement in response to a crisis. In addition, the Department of the Treasury—along with the FBIIC, the FSSCC, Financial Services Information Sharing and Analysis Center (FS–ISAC), and regional partnerships—have developed and continue to implement numerous protective programs to meet the Financial Services Sector's goals. The protective programs range from developing and testing robust emergency communication protocols, to identifying critical Financial Services Sector threats, to addressing cybersecurity protection needs. The success of the public-private partnership has proven critical to the Financial Services Sector's achievements through one of the most challenging periods for the sector with respect to credit and liquidity risks.

The scope of the Financial Services Sector includes public and private institutions involved in carrying out the primary sector functions of clearing, payment, settlement, and trading. Multiple organizations perform these functions and collectively represent the Financial Services Sector.

- Clearinghouses
- Commercial banks
- Credit rating agencies
- Exchanges/electronic communication networks
- Financial advisory services
- Financial utilities
- Government and industry regulators
- Government subsidized entities

- Investment banks
- Merchants
- Retail banks
- Insurance companies
- Electronic payment firms

Through the public-private partnership, the following vision statement for the Financial Services Sector has been established.

"Vision Statement
"To continue to improve the resilience and availability of financial services, the Banking and Finance Sector will work through its public-private partnership to address the evolving nature of threats and the risks posed by the sector's dependence on other critical sectors."

The Financial Services Sector pursues this vision by working toward its three sector goals:

1. To achieve the best possible position in the face of myriad intentional, unintentional, manmade, and natural threats against the sector's physical and cyber infrastructure;
2. To address and manage the risks posed by the dependence of the sector on the Communications, Information Technology, Energy, and Transportation Systems Sectors; and
3. To work with the law enforcement community, financial regulatory authorities, the private sector, and our international counterparts to address threats facing the Financial Services Sector.

In support of the sector goals, the FSSCC has recently updated its mission and objectives, as is further described in Section 3. Representing the strategic arm of the Financial Services Sector, the FSSCC has established the following objectives:

- Identify Threats and Promote Protection
- Drive Preparedness
- Collaborate with the Federal Government
- Coordinate Crisis Response

The Financial Services Sector's goals and objectives guide our activities in managing significant sector risks. Significant sector risk considerations have been identified and are described in greater detail in Section 2. They are summarized as follows:

- Confidence Risk
- Concentration Risk
- Supply Chain Risk
- Infrastructure Risk
- Geographic Proximity Risk
- Technology Risk

Management of these risks has resulted in the identification of the following potentially significant sector vulnerabilities:

1. Confidentiality.—Maintaining the confidentiality of clients and meeting all legal requirements for maintaining confidentiality;

2. Integrity.—Ensuring transactional integrity to support financial transactions; and

3. Availability.—Ensuring that financial services are available to maintain the smooth flow of capital.

The sector's goals, initiatives, and activities are in pursuit of achieving the four objectives identified above to effectively manage sector risks and vulnerabilities.

The following sections summarize the significant activities that are described in subsequent chapters of this Financial Services Sector Annual Report.

ES.1 Strategic Goals

Over the past year, the Financial Services Sector set forth the following objectives and goals that drive the FSSCC activities and guide activities of the sector's multiple organizations.

Strategic Objectives	2010 Goals
Identify Threats and Promote Protection.	Finalize updated Threat Matrix. Disseminate Threat Matrix and build into strategy. Build Threat Matrix into ongoing planning and execution of FSSCC goals.
Drive Preparedness	Establish regularized process for escalating events and disseminating information in the form of actionable intelligence. Establish more direct international relationships. Further the undersea cables work. Develop supply chain frameworks. Disseminate CyberFIRE and Cyber Attack against Payment Processes (CAPP) Exercise learning. Support regional coalitions.
Collaborate with the Federal Government.	Establish on-going interaction with (1) the new White House Cybersecurity Coordinator and (2) DHS/National Security Agency (NSA). Address internet congestion as part of DHS interaction. Develop Identity Management Principles and request for investment. Implement Government Information Sharing Framework initiative with Department of Defense (DoD) and DHS. Develop sector-wide position on Internet Corporation for Assigned Names and Numbers (ICANN). Engage in conversation on cyber and critical infrastructure legislation and determine appropriate next steps. Deliver a finance and banking educational session.
Coordinate Crisis Response	Expand and improve crisis management response playbooks. Improve usefulness and mindshare of playbooks.

ES.1.1 Identify Threats and Promote Protection

The Financial Services Sector is developing a comprehensive All-Hazards Threat Matrix accounting for over 1,900 individual threats. A risk-ranking methodology is being used that can be applied at the sector level and adopted by individual organizations to adapt to their specific needs. As a major initiative for the sector, begun in 2009, it will continue throughout 2010 and serve as the foundation for strategic efforts going forward.

Additionally, the sector published the *Resilient International Telecommunications Guidelines for the Financial Services Sector* (Undersea Cables Report), highlighting the international risks associated with our undersea cables network. This significant report highlights both the risks associated with a critical infrastructure component and the need for increased international collaboration.

Additionally, the sector has elevated its focus on cybersecurity. Several exercises have been run to identify cyber threats, and research and development (R&D) efforts have been focused on addressing vulnerabilities through a collaborative public-private joint effort. The sector made significant contributions to the National Cyber Incident Response Plan, created new FSSCC working groups focusing on Identity Management and Supply Chain issues, and engaged with the Director of National Intelligence and the intelligence community on multiple cyber issues.

ES.1.2 Drive Preparedness

The sector has performed multiple exercises testing various perceived vulnerabilities and establishing follow-up actions as a result of the learning. Significant tests were run to evaluate sector preparedness related to social engineering attacks, payment processing attacks, and communication during a crisis. In particular, the Cyber Financial Industry and Regulators Exercise (CyberFIRE) and Cyber Attack against Payment Processes (CAPP) Exercises were jointly executed by the FSSCC, FS–ISAC, and FBIIC and included the U.S. Secret Service, the Federal Bureau of Investigation (FBI), and the U.S. Department of Homeland Security (DHS), plus more than 800 individual participants.

Sector crisis response playbooks have been created and strategic and tactical efforts have been delivered to clarify lines of communication critical in crisis response.

The sector coordinated over 45 operators and associations and performed multiple other FS–ISAC and regional exercises throughout the year.

ES.1.3 Collaborate with the Federal Government

The Financial Services Sector has stepped up its partnership with the U.S. Government, academia, and related sectors. The sector has established successful working relationships with academia, the National Institute of Standards and Technology (NIST), the Department of Homeland Security, the National Science Foundation (NSF), and the Networking and Information Technology Research and Development (NITRD) program; participated in a roundtable with the DHS Secretary; and established a working dialogue with the White House's Office of Science and Technology Policy (OSTP) through Aneesh Chopra.

The sector has further contributed significantly to Government-led initiatives in identity management and the development of incident response plans. Coordination among intelligence agencies, regulators, other Government agencies, and the private sector has received considerable focus and is a hallmark of the sector's achievements.

The FS–ISAC has collaborated with DoD and DHS to launch the Government Information Sharing Framework initiative. This pilot program has been implemented in 2010 and consists of large-scale information sharing of threat and attack data between the Federal Government and financial services firms that have agreed to participate. The Government's plan is to use this as a public-private sector information-sharing model for other sectors and other Federal Government agencies to follow.

ES.1.4 Coordinate Crisis Response

The sector collaborated to develop crisis response plans for all hazards, as well as specific plans for hurricanes. The sector provided leadership for recent events requiring a coordinated response, including Haiti, pandemic flu, and hurricane situations.

ES.1.5 Conduct Research and Development

Led by the FSSCC R&D Committee, the sector has identified and progressed on seven R&D priorities it has established (further described in Section 5):

- Advancing the State of the Art in Designing and Testing Secure Applications
- Making Financial Transaction Systems More Secure and Resilient
- Improving Enrollment and Identity Credential Management
- Understanding Human Insider Threats and Developing Deterrence and Detection
- Developing Data-Centric Protection Strategies to Better Classify and Protect Sensitive Information
- Devising Better Measures of the Value of Security Investments
- Developing Practical Standards to Reduce Risk and Enhance Resiliency.

The FSSCC R&D Committee has proposed to senior White House and other Government officials a public-private sector collaboration to improve identification validation and has drafted a proposal on an identity credential verification gateway. Further, it participated in the Federal Government's National Cyber Leap Year Summit and put forth the Financial Communications and Authentication Pilot ("testbed") in response to discussions among the FSSCC R&D Committee, senior White House personnel, and NIST and DHS officials.

Outreach for R&D efforts has been significantly expanded. Several comment letters have been sent, and engagements have occurred with multiple Government organizations, including the U.S. Department of State on "Current Challenges and Future Strategies for Improving Identity Management," the Critical Infrastructure Protection Congress on identity management, and the Internet Corporation for Assigned Names and Numbers (ICANN) on the expansion of top-level domains, among others.

ES.2 Sector Challenges and Looking Forward

Looking forward to the next year, the Financial Services Sector will build on its substantial success achieved in the past year. While priorities will be set later in the year, significant efforts are expected to focus on the following:

- Evaluating the top threats to the Financial Services Sector
- Coordinating multiple Government activities
- Researching internet congestion
- Investigating ICANN proposals to expand top-level domains
- Exploring identity management issues
- Expanding international coordination.

Mr. LUNGREN. Thank you very much.

Now Dr. Amoroso.

STATEMENT OF EDWARD AMOROSO, SENIOR VICE PRESIDENT AND CHIEF SECURITY OFFICER, AT&T

Mr. AMOROSO. Well, thank you very much.

This is a topic I have spent the last 30 years thinking about exclusively. So I am not a lot of fun at cocktail parties. But it is something that I know a fair bit about.

Let me see if I can boil down the fundamental issue of cybersecurity in particular as it relates to homeland security. It is something that I think people can pretty well understand. That is how you protect your home computer.

Like if I had asked everybody in the room to take a moment and think about what you do at home, you probably went to Staples or something and bought, you know, a box of internet security or it came with the computer. You enabled it, and that is pretty much it. You are completely on your own. Like you might call the Geek Squad if you get in trouble, or you might have a really smart teenager in the family who can do something if you get hopelessly tangled up. Or you might just give up and go buy a new computer, right, if you think that you are full of malware and other types of things.

This experience that we all have at home is exactly the experience that small businesses and Government agencies and large businesses have as well. We go out and we buy software and systems that we hope are going to work, and then we are pretty much on our own. I know in each of the districts that you represent, you probably hear that from small business owners all the time. Citizens are starting to recognize that this is an issue.

I think from a homeland perspective, this causes a big problem, right, because, as you all know, the new battlefield that we work from a cyber perspective includes all our home PCs, right? That is how botnets are created. We are in some sense kind of negligent in protecting our PCs, and criminals and terrorists and enemy states take advantage of that and create weapons in that respect.

So we have prepared some formal remarks that we have issued that have some suggestions, but I just want to summarize a couple of them.

If you think about that question of coordination, like when a group is under attack, it is the case now in 2011 that there is no good way to share information in real time. I know that at AT&T, for me to try to do something like that with Government involves as many lawyers as there are in this room for us to just share something. It is ironic that I can probably share information back and forth with a hacking group with complete impunity, but with the Government I have to have a team of lawyers present.

So that concept and the whole issue of a National sort of cyber coordinating capability that has real-time information sharing— and I don't mean after the fact. I mean something that would allow us in real time to share and to coordinate.

Let's say you are in Brooklyn and you are living and you see something funny going on that you are not sure is normal in your neighborhood. We are all kind of trained to kind of take action. You can imagine that a nation of businesses and agencies and individuals who in some sense have it in their best interest to behave accordingly and to share that information would make us all a heck of a lot safer.

There really is no mechanism for that. I know at AT&T sometimes we find that kind of frustrating. Because we have information that may be very useful at times to DHS, and we know DHS does as well. I think the NCCIC is a good example of moving in the right direction toward trying to sort of connect different groups together. But I think the essence of real time, the essence of situational awareness, these are things that are very immature in our country right now.

I would add, you will see in the remarks that we have prepared for the group, it extends to global as well. It turns out that political boundaries don't map too nicely to cybersecurity infrastructure. There are ways that we do naming, for example, on the internet, the way you get your website named or your e-mail address named. These are global standards, and they run on systems that transcend political boundaries. I have infrastructure at AT&T that is located around the globe, under different jurisdictions with different laws. So even if we got our act together and really laid out a good domestic plan, it is not enough. We have to go out and work it globally.

So I hope you will read our prepared remarks. We make some suggestions there. But keep in mind that the challenge you have at home with your home PC is a good model for the kinds of problems that Government agencies and businesses have as well.

So I appreciate the invite and look forward to the discussion.

[The statement of Mr. Amoroso follows:]

Prepared Statement of Edward Amoroso

April 15, 2011

Chairman Lungren and Ranking Member Clarke, I would like to thank you and all the Members of the subcommittee for this invitation to address the significant challenges facing the private sector and the Department of Homeland Security in securing critical infrastructure from cyber threats. In my testimony, I will try to identify current challenges as well as the actions that can be taken to address those challenges; and in particular how to coordinate the Government's cybersecurity capabilities with the private sector's investment in infrastructure and operational capabilities.

MY BACKGROUND

I currently serve as senior vice president and chief security officer of AT&T, where I have worked in the area of cybersecurity for the past 26 years. My educational background includes a Bachelor's degree in physics from Dickinson College, as well as Masters and Ph.D. degrees in computer science from the Stevens Institute of Technology, where I have also served as an adjunct professor of computer science for the past 22 years. I am a graduate of the Columbia Business School, and have written many articles and five books on the topic of cybersecurity. My most recent book is entitled "Cyber Attacks: Protecting National Infrastructure" (Butterworth-Heinemann, 2011).

My current responsibilities include design and operation of the security systems and processes that protect AT&T's vast domestic and international wired and wireless infrastructure. This infrastructure is the core asset that permits AT&T to provide the wide variety of advanced network services that AT&T offers to its many millions of customers around the world, ranging from the largest global business enterprises to individual consumers. AT&T has also had the opportunity to work with the Department of Homeland Security (DHS) in a variety of ways in the decade since the Department was created.

For instance, we actively participate with DHS in the National Cybersecurity Communications Integration Center (NCCIC) in both its National security/emergency preparedness and cybersecurity missions. We are also active participants in the President's National Security Telecommunications Advisory Council (NSTAC) and the Communications Sector Information Sharing and Analysis Center, both of which are administered by DHS. We have also supported DHS in the testing and evaluation of prototype network-based cybersecurity capabilities over the last several years. Finally, we were the first company to obtain a formal Authority-To-Operate to provide Trusted Internet Connection service to Government Agencies through the General Services Administration (GSA)/DHS joint Managed Internet Protection Service initiative under the GSA Networx contracts.

WHAT IS CYBERSECURITY?

Simply put, from the perspective of protecting the Nation's critical infrastructure, cybersecurity is the ability to protect critical systems from disruption, or critical information from alteration or theft. Potential threats range from disgruntled individuals to criminal elements to transnational actors to sophisticated and well-resourced nation states. Motives can range from mischief to deliberate acts of hostility through sabotage and terrorism. The methods and forms of infrastructure intrusion are continually advancing so as to bypass standard preventive measures such as the application of firewalls and intrusion detection systems between the critical system and the internet at large. One such form of evolving cyber attack uses "botnets"—which are run by malicious parties who are increasingly adept at harnessing the power of dispersed personal computers and other smart devices attached to the Nation's networks and using them to attack unsuspecting victims.

As the largest provider of communications and network services in the world, AT&T takes very seriously its responsibility to protect our infrastructure and our customers from the vast and ever-changing cyber threats. Cybersecurity is a business imperative at AT&T, and we work very hard at it, investing significant resources to innovate and keep pace with technology that may be either the source or target of the threats. The size and scope of AT&T's global network, coupled with our industry-leading cybersecurity capabilities, gives AT&T a unique perspective into malicious cyber-activity. AT&T offers one of the world's most advanced and powerful global backbone networks, carrying 23.7 Petabytes of data traffic on an average business day to nearly every continent and country (a Petabyte is a million billion bytes of data, or a "one" followed by 15 zeros), and we expect that to double every 18 months for the foreseeable future. Our intelligent network technologies give us the capability to analyze traffic flows to detect malicious cyber-activities, and in many cases, identify very early indicators of attacks before they have the opportunity to become major events. For example, we have implemented the capability within our network to automatically detect and mitigate most Distributed Denial of Service Attacks within our network infrastructure before they affect service to our customers, and we continue to improve our ability to provide global coverage to mitigate denial-of-service attacks from multiple locations across the United States, as well as nodes in Europe and Asia. We are constantly improving our cyber capabilities, including the ability to detect and mitigate Advanced Persistent Threats, the most sophisticated and pernicious forms of cyber attack.

WHAT NEEDS TO BE DONE?

I would like to outline four broad themes for your consideration during today's hearing. Improving the overall cybersecurity posture of the United States is a daunting task. We cannot undertake this challenge unilaterally—it is clearly a global issue in all its dimensions. The administration and the Congress have put forth a variety of ideas and initiatives on how we can begin to tackle this challenge; some are helpful, and some would stifle the innovation and flexibility we need to identify and respond to the ever-changing threats. Improving our National cybersecurity posture is a long journey that will not be solved by simple pronouncements or regulatory dictates. We can, however, start to put some foundational elements in place to build on for the future.

1. Build a Collaborative Active Cyber-Defense Capability.

First and foremost, the United States needs to build a collaborative active cyber-defense capability. The global communications infrastructure is the primary vehicle for delivery of cyber attacks against U.S. interests, yet there is no comprehensive coordination mechanism for rapidly detecting and analyzing attacks and responses.

Each Tier One communications network operator and service provider monitors its own network to varying degrees, with varying capabilities to mitigate or block attacks. In addition, the multiple Government programs which already exist are focused on monitoring traffic to and from multiple Government networks—none of which are operationally integrated. Given the increasing sophistication and scope of cyber attacks, we can no longer expect that individual companies or consumers, or disparate Government network monitoring programs, provide adequate protection against evolving threats.

Attack-related protective information might be known to the Federal Government, for example, but otherwise unknown to private industry. In the event that a Government agency becomes aware of a malicious attack signature that could be deployed into intrusion detection systems to protect industrial, non-Government assets, the Government should have the confidence that it can be so deployed without further delay or review. A collaborative active cyber-defense capability to detect, analyze, and mitigate malicious cyber activities in the core networks that make up the internet itself will enable cyber attacks to be detected and attempts be made to stop them before they reach their target.

Such a capability should leverage and build upon the existing cybersecurity capabilities of the Tier One network operators and service providers whose networks are the core of the internet in the United States, as well as the complimentary capabilities of the security technology and software industries. Critical National systems, large and small business, industrial concerns, and individual internet users can all be better protected by this umbrella approach. Combining these elements to work in a collaborative and coordinated fashion can provide the basic foundation for the active cyber-defense capability. National intelligence capabilities to identify cyber threats and provide advanced warning can also be leveraged. In this way, a new collaborative cyber defense capability will both feed into and strengthen existing public-private coordination and response efforts.

2. Government Leadership in Acquisitions and Cyber Management.

The United States Government should lead by example in cybersecurity. The Federal Government is the largest single purchaser of information technology and network services in the United States, and its leadership and buying power can have great influence on the cybersecurity marketplace. Several worthwhile Federal initiatives are in place to improve cybersecurity for the ".gov" domain, such as the Trusted Internet Connection effort by the Office of Management and Budget (OMB) and its instantiation via the General Service Administration/Department of Homeland Security joint initiative on Managed Trusted Internet Protection Service, but they are being applied inconsistently. The Department of Defense also has its own effort to protect ".mil", separate from the ".gov" efforts. These initiatives do not yet take full advantage of the portfolio of managed security services offered by many private sector network service providers, such as network-based protection against Distributed Denial of Service (DDOS) attacks. The Federal Government needs a clear and comprehensive strategy for cybersecurity of all Federal systems which make up ".gov" and ".mil"—one which effectively leverages existing cybersecurity capabilities offered by the network service providers.

Further, the current roles and authorities of the various Federal agencies overlap and are unclear with respect to cybersecurity for Federal Government infrastructure, as well as the protection of other critical infrastructure, National assets and individual consumers. Congress can lead by establishing the respective and definitive roles and authorities of the various Executive Branch elements involved in all aspects of cyber security—including the National Security Council and the Cyber Policy Coordinator, the Office of Management and Budget, the Office of Science and Technology Policy, the Department of Homeland Security, the Department of Commerce including the National Institute of Standards and Technology and the National Telecommunications and Information Administration, the Department of Defense including U.S. Cyber Command and the National Security Agency, the Department of State, the Federal Communications Commission, and the Federal Trade Commission. The United States needs a unified Federal effort on cybersecurity with a clear understanding of the roles involved—not the confusion, inconsistency, and overlap that currently exists.

3. Global Strategy.

The United States must move forward aggressively to create a comprehensive strategy for addressing global cooperation in cybersecurity. We must reinforce the leadership of the United States in shaping the future of the internet, and assuring its stable, reliable, and secure operation, concurrent with the expansion of U.S. enterprise in the global internet marketplace. In particular, all members and participants of the global internet community must achieve consensus on the fundamental point that malicious cyber activities of any sort will simply not be tolerated. Concurrent with these efforts, Congress should also expand incentives for investment by the private sector to help invigorate U.S. technology leadership in cybersecurity and the internet.

4. Cyber literacy.

We all must redouble our efforts in cybersecurity education and awareness across the full spectrum of the internet user base—from the boardrooms of our largest companies to the millions of individuals who surf the 'net. Current efforts in cybersecurity education and awareness are fragmented and the messaging is often confusing. The ultimate key to improving our National cybersecurity is technology innovation driven by market demand from informed users and purchasers of all kinds. By creating market demand for cybersecurity through heightened consumer awareness, we can spur fundamental security innovation at all levels of the internet eco-system, and allow the United States to continue as a leader in internet development. To that end, Congress should designate a lead agency on cybersecurity education, and support that designation with an appropriate level of funding to make it effective. The roles of other Federal agencies in supporting this effort should also be clarified. AT&T is itself actively engaged in the provision of cybersecurity information and protective tools to our customers, and actively participates in pan-industry cyber awareness education efforts such as "Stop.Think.Connect," the coordinated messaging effort spearheaded by the Anti-Phishing Working Group and the National Cyber Security Alliance and comprised of Government agencies, private sector entities, and not-for-profit corporations.

In the past, cybersecurity legislative proposals have included a variety of regulatory schemes, such as certification regimes, that, while well-intentioned, are too often the antithesis of innovation—such requirements could have an unintended stifling effect on making real cybersecurity improvements. Our cyber adversaries are very dynamic and ever more sophisticated, and do not operate under a laboriously defined set of rules or processes. The challenges we face in cybersecurity simply cannot be solved by imposing slow-moving, consensus-based bureaucracy on those who build, operate, and use cyber space. Overbroad regulation and certification requirements can have unintended consequences, such as emphasizing the status quo by focusing on yesterday's challenges. An overly prescriptive approach can only serve to stifle internet innovation and the technology leadership of the United States in the global information infrastructure.

The internet itself was created through innovation. Some key early investments by the Government helped spur that innovation. Congress and the administration have leadership roles to play in assuring that the United States continues to focus on technology innovation. Burdening the private sector with the cost of unnecessary and ineffective regulations and processes is contrary to that objective, and will only slow advances in cybersecurity. Congress must insist on and support initiatives that provide the flexibility needed to deal with the dynamics of the threat and the technology, while creating innovation and investment through market demand.

I thank the subcommittee for its timely and focused attention on cybersecurity, and I look forward to providing on-going guidance, assistance, and recommendations as we collectively work to reduce the cybersecurity threat to our Nation and our critical infrastructure.

Mr. LUNGREN. Thank you very much.

I thank all the panelists for your testimony.

We will go into a round of questioning of 5 minutes a piece, and I will start with that.

Dr. Amoroso, in your testimony you talked about if we were to have enhanced market demand for cybersecurity through heightened consumer awareness that might be an element to help us along the way in creating those kinds of mechanisms necessary from the ultimate consumer to major corporations.

This is one of the things that has always been presented to me. How do we make it bottom-line relevant for both individuals and businesses? Because when you say increasing consumer awareness will lead to that, that presumes that people will be aware enough to spend the money to do those things that are necessary and to spend the time to take those simple steps that would be necessary to engage those systems that they have on a regular basis.

Do you have any suggestions about how we do that, particularly with corporations so that corporations—look, in the financial services industry and in the communications industry, I think it is fairly more self-evident to people that, bottom line, it is important. Cybersecurity destroys your very product, your very service.

In others, they might hedge and say, well, the chance that someone is going to attack me in a way that is really going to hurt me may not be that great. If they really do succeed, that would hurt me, but the chances of them doing that are not very great. So how can I justify that to my shareholders?

Could you give us some insight on that?

Mr. AMOROSO. Well, one thing Government can do is lead by example. Certainly I think a lot of the cybersecurity mechanisms that are laid out, say through GSA and DHS and other places, are applied pretty unevenly. I know that my team owns and operates infrastructure in support of the GSA network's MTIPS program, which is a trusted internet connection. I will say that it is applied somewhat unevenly. There are some excellent services that GSA provides, data analysis service, real-time capabilities for making sense of what is happening on a given network.

I think that one of the responsibilities of Government is to look first inward at civilian and defense and other types of agencies, even State and local to the degree that we have that kind of jurisdiction, and to show by example that not only is this important but it can actually be done.

There are two problems. One is, a lot of groups—to your point—don't necessarily see it as urgent. But perhaps more troublesome, even if they saw this urgent, they are not really sure what they should even be doing, right, just as you would at home.

If I convinced you tomorrow that identity theft was the most important thing in your life, how would your PC usage change? You would probably shrug and say, all right, I am a believer. What do I do?

We start these things by saying how complex a problem it is. Here is one of the dimensions that makes this particularly troublesome for this committee. Once we get our arms around some techniques that seem to work, the technology has already changed.

I am guessing most of the people in here have a Smartphone in their pocket. That is an internet-connected computer that you have in your pocket that probably has more power than a data center had when you started your career, and now you carry it around with you in your pocket. Just graph that out another 10 years, and that is the threat that we should be planning for now, not the threat that exists today. It makes it extremely difficult, because the technology changes so dramatically.

So, again, cooperation, coordination, those are the types of things that we really need to foster. Because the hacking community seems to do that maybe even better than we do as a Federal Government.

Mr. LUNGREN. Ms. Carlin, if you could respond to that. Also, you made some suggestions about how we might be able to improve some things in a coordinating council. Part of that is relationship building. You can have it all in the schematic, but unless people have trust that they can share information they won't do that and not even get to Dr. Amoroso's point about how you make it in real time. Could you just comment first on the bottom-line relevance and then secondly about specific improvements maybe we need on the Government side with respect to a coordinating council?

Ms. CARLIN. Sure. Thank you.

As to the first question, I guess I think of it a little differently maybe than Dr. Amoroso in the following sense: Many of the institutions that make up the financial services marketplace, including the critical infrastructure components we depend on, are then each regulated often by different regulators. Many of the regulators in financial services already have robust standards around data security principles and standards they expect the banks and other regulated entities to observe.

Where I think there is really a significant remaining gap is in what I think of as utility standards. There are utilities operating that constitute critical infrastructure assets who themselves are not subject to baseline minimum standards related to data security.

Now I don't think of that, quite frankly, as regulation or legislation, for that matter but, rather, baseline minimum operating standards, recognizing the interconnectedness and interdependence that we all have. A failure of one represents a failure of all, and we have seen it over and over and over again.

As to the second question and our specific recommendations, what we are recommending is a documented protocol that will provide a more regularized and repeatable process to the decision of when to disclose information to the community. So rather than making it up each time as we go along and treating it almost as an artist's project, let's inject some science into that question. What are the considerations that the law enforcement, intelligence, regulatory, and private industry communities bring to bear when an event happens? How do we appropriately balance, as an example, the importance of an on-going investigation with the public policy considerations related to disclosure? The event that I refer to in my testimony, the 102-day delay, cut across fiscal year end for the vast majority of public companies in the United States. How did we do that without this information?

Mr. LUNGREN. Thank you very much.

I recognize now for 5 minutes the Ranking Member from Brooklyn.

Ms. CLARKE. Thank you, Mr. Chairman.

Mr. McGurk, you have told my staff on previous occasions that when your office conducts analysis of control systems in critical infrastructure sectors, such as the electric sector, they often report to you that those systems are air gapped or physically separated from their business system. But, in fact, when you check their system, that is almost never the case. Can you tell us about that, please? Is it your experience that, once this is pointed out, that the companies fix the problem or do they just ignore it? Are there other sectors where this is the case?

Mr. MCGURK. Yes, ma'am. Thank you very much for that question.

Indeed, the results of our on-site assessments as well as our incident and response events have identified that in no case had we ever found a situation where the operations network and enterprise networks were fully air gapped. There were always types of connections and, for many systems, very good reasons why they are connected. The challenge runs the gamut of service-level agreements, regulatory reporting requirements, or other information-sharing information. So there are good reasons.

What we found is that not necessarily is there a good cyber hygiene approach to securing those communications networks or those nodes. There is technology available which provides unidirectional flow of information that cannot be breached so that they could put processes and procedures in place to prevent the flow of information or preventing a malicious actor from coming back into those networks and those systems. So those technologies are out there, and they have been analyzed, and they have been validated by various members of our National lab complex.

We work closely with the private sector in identifying those vulnerabilities. Once we do, in every case, the asset owners and operators have taken necessary and proactive steps to close or mitigate those vulnerabilities by actually incorporating new procedures or new technology to mitigate that risk. The private sector has been very responsive in complying with those requirements and those necessary risk mitigation strategies.

Ms. CLARKE. So in speaking with the sector now that that has been identified, has there been a new terminology that is utilized? Because I mean I am just trying to think of the mindset that would believe that, you know, they have got this air gapped situation in place and not really acknowledging the vulnerability that exists because of the connection. Has there been a change in thought from your perspective in working with the sector?

Mr. MCGURK. In each case, in several sectors that we have worked with and many of the sectors are being proactive about it, they are focusing on trusted connections, as opposed to no connections. People recognize that there is a need for the connections, but they must be trusted connections. There are a number of industry and Federally identified standards which focus on increasing that level of security and that level of trust.

So, yes, ma'am, they are certainly taking those necessary steps.

Ms. CLARKE. Wonderful.

Mr. Cauley, it is good to see you again; and thank you for participating in the Electric Infrastructure Security Summit on Tuesday. Your contributions were very valuable, and your presence here today is very important as well.

I want to follow up with you on the question I just asked Mr. McGurk. Do you recommend that critical control systems be air gapped? What are some of the recommended or required approaches? How are you ensuring that the electric sector companies are putting them in place? I think this sort of goes to Ms. Carlin's point with respect to the financial sector. It is the utilities that I think we are all relying on as part of an ecosystem, if you will.

Mr. CAULEY. Ranking Member Clarke, I think you have really hit on a really critical issue. The challenge is the power system, if you look at it from the bulk power all the way down to the meter, is everywhere. There are hundreds of thousands of substations. We are distributed on down every street and every corner. So the concept of air gapping the power system is really a conceptual one, and I think it has merit, and we are looking at it.

I agree with most of the comments of Mr. McGurk. I think the awareness of the industry has improved. There have been efforts. You have vendors or employees who can dial in remotely and access equipment to do maintenance and special tasks.

The number of those ports have been reduced. The number of interfaces between the control systems and the business systems have been reduced. I think there is a general awareness. But to say we could air gap the power system is really challenging just because of the hundreds of thousands of locations and computers and equipment. So I think we have to challenge ourselves.

Also, there is an enormous dependency between operating the power grid and the communications that underlie it. Many of the companies depend on telecom companies, phone companies for the wires that connect the communications between the power grid stations. So it is an important issue.

Can we get to an air-gapable power system or an electric system? I think we are a ways away from that. Right now, we are prioritizing on critical assets and making sure they are firewalled and protected and that we have proper protocols.

I think the issue of one-way data communications is new. We are pressing to get that more widely used in the industry.

Thank you.

Ms. CLARKE. Thank you, Mr. Chairman.

Mr. LUNGREN. Mr. McCaul from Texas is recognized for 5 minutes.

Mr. MCCAUL. Thank you, Mr. Chairman.

I am not Mr. King. I just wanted to see what it felt like to be King for a day. I hope Pete is not watching this hearing. It feels good.

Let me thank the witnesses for being here.

We have had hearings on the dot-mil and the dot-gov; and today's hearing, in my judgment, is on the dot-coms and how do we protect the private sector that controls a majority of the critical infrastructures? What can the Government do and what can we do in Congress in terms of the legislation? I think there is some legislation out there—our first credo should be to do no harm. I think sometimes we legislate, and there is a law of unintended consequences, and I will get to that in a minute.

I remember working at the Justice Department, with the FBI, and then the ISACs came around, and they have been around for about a decade. We are still not there, in my judgment, with the ISACs in terms of full—Dr. Amoroso, as you mentioned—full real-time information sharing.

You made a comment that I wanted to follow up on that, thought it was real interesting, that you need a team of lawyers to talk to the Government. I know there is a FOIA exemption for critical infrastructure sharing, but I don't know if that is always applied or if that exemption always attaches to that information sharing. But could you elaborate, Doctor, on that point that you made?

Mr. AMOROSO. This is a concept I know you are aware of, signature. So somebody figures out that there might be an attack, and if you look for this particular file or this command or some little tip that would help either an operator or a government or anybody figure out that this attack is going on, it is sort of the currency that we all work in. That is how we tip each other off in cybersecurity. We provide signatures.

For the Government to provide a signature to a carrier that we would then embed into our services to protect customers and so on and so forth, there is a tremendous lack of clarity around whether that is legal or not or whether we would be operating as an agent of the Federal Government or whomever.

As I sort of joked, if I am wandering around a hacker conference and somebody gives me the same information, not in Government, some hacker dude with a Grateful Dead t-shirt on or something, I pop it right into our infrastructure and everything works great. So that lack of clarity, it really points to the fact that, depending on which attorneys you are talking to or which person, some might say, oh, no, no, no, no, you can't do that. Others would say, no way can you do that. I work for a very conservative firm, so we are going to err on the side of not doing it. So we need clarity there.

Mr. MCCAUL. That is an interesting point. Mr. McGurk, how can we fix that? What would you propose? I assume we are going to be legislating cyber out of this committee, subcommittee. What would you propose?

Mr. MCGURK. Yes, sir. Actually, we are currently sharing that information with our private-sector partners but not insofar as signatures. Because, going back a bit, a signature is specific to whatever box—to use the analogy—that you pulled off the shelf at Staples. It may be system-specific or product-specific.

So what we can share and derive are the smaller part of that called indicators, and we publish those indicators routinely. Those indicators can then be taken by the technical representatives of each of the facilities or firms and generate those signatures that then are specific to those pieces of equipment. So we are currently doing that.

In fact, in light of the recent situation with the two-factor authentication issue, we produced about 26 indicators that asset owners and operators could then load into their systems to look for malicious activity. So it is a very complex but multi-pronged approach that we are taking to provide actionable intelligence to the community.

Mr. MCCAUL. I agree with Dr. Amoroso. I think clarity would be helpful, whether that comes through legislation or through policy within the Executive branch.

But, lastly, just to throw out there, how do we incentivize the private sector to harden its networks? AT&T, certainly you guys are ahead of the curve, but a lot of companies aren't. There is the Senate bill which is very comprehensive. It has DHS regulating the industry. I personally don't agree with that legislation. But how can we incentivize the private sector to harden their networks?

Mr. MCGURK. Sir, I believe a comment was made earlier that we can lead by example, and that is one of the areas that we are really looking to focus on both at the National and at the Federal and international level, is how can we provide guidelines and steps? The Department actually publishes and updates on a quarterly basis procurement standards for asset owners and operators that are buying new technology or incorporating new pieces of equipment. In addition, we write a comprehensive guide for standards developers so that they understand what the market is driving as far as requirements.

So by providing that and also identifying best practices through either Federal standards or industry adopted standards, we can identify what a network topology can and may look like to increase security.

But, again, it is more descriptive in nature, not proscriptive. Because no one network or network configuration is going to operate—an automobile manufacturing plant, a chemical processing facility, or a nuclear power plant, they are all unique and different, which is why we have to take a very sector-specific approach.

Mr. MCCAUL. That is a good point.

I yield back.

Mr. LUNGREN. The gentlelady from California, Ms. Richardson, is recognized for 5 minutes.

Ms. RICHARDSON. Thank you, Mr. Chairman.

I have got five questions, so hopefully we can get through them pretty quickly.

Mr. McGurk, what would you rate as the rating for DHS when you hosted your Cyber Storm III exercise?

Mr. MCGURK. As far as an opportunity to learn and to explore, I would say it was probably, on a scale of 1 to 10, about a 7. Because we had a very large play this time with both of our State partners, private-sector partners, and international partners. We learned a lot of important lessons, and this was actually the first time we got to exercise the National cyber incident response plan and execute it in accordance with the system and the NCCIC. So it really helped us out.

Ms. RICHARDSON. Have you briefed this committee on that yet?

Mr. MCGURK. I don't believe so, ma'am, but I would have to check with our team back at headquarters.

Ms. RICHARDSON. If not, if you would work with Mr. Lungren and with our staff and hopefully maybe we could get some further information on it.

No. 2, do you think the NCCIC, which is your organization, should be voluntary with the private sector?

Mr. MCGURK. It is currently voluntary with the private sector, ma'am. We have——

Ms. RICHARDSON. I said, do you think it should be voluntary? Or should it be mandatory?

Mr. MCGURK. I am not really sure what you mean by voluntary versus mandatory. As far as participation, we open it up to the broad sectors. Each of the sectors have the potential of being represented, but the products that we produce and the information that we share goes to the broad community. So we do not restrict it in any way.

Ms. RICHARDSON. No. What I mean is, the private sector—let's take, for example, AT&T. Although it is a private company, you know, has its own business, it is still providing a very important service that we, as the American public, expect to be able to use our phones in the event of an emergency. I am saying, has there been a discussion ever that maybe your role would need to be a mandatory or a more formal relationship versus voluntary involvement?

Mr. MCGURK. No, ma'am. At the present, we are not looking at that particular type of involvement. AT&T has been represented in the National Coordination Center for Telecommunications since its inception as well as the NCCIC since October, 2009. So they have been a direct partner with us since the beginning of the organization.

Ms. RICHARDSON. Are there any industries that you have felt you needed to work with that you currently don't really have the authority and the ability to do so?

Mr. MCGURK. No, ma'am. Each of the sectors have been very responsive and receptive to coordinating, sharing information, and receiving information from the Department.

Ms. RICHARDSON. Okay. Within your voluntary public-private partnerships, how many would you say are corporation size, midsize, small business, if you could give a percentage of who you work with.

Mr. MCGURK. It is actually very broad. We work with Fortune One companies, the large carriers, and the large manufacturing facilities here in the United States, all the way down to small companies which employ only seven employees.

Ms. RICHARDSON. But of those that you work with, what would you say would the percentage be? So would you say corporations, you spend 50 percent of your time and small business 10 percent? What is kind of a percentage?

Mr. MCGURK. It is more of a broad range. I would say that we spend 100 percent of our time within each of the sectors focusing on, from the small community up to the large community. In the case of developing mitigation strategies and plans, we are looking more for the subject matter expertise, not necessarily at what level they reside. So we do try to focus across the board a very broad spectrum.

Ms. RICHARDSON. Okay. How many approximately in your private sector have you worked with, approximately? One thousand? Two thousand?

Mr. MCGURK. It is very hard to quantify, ma'am. I would have to get back with you on that type of number.

During the last mitigation development process, we had over 50 companies from six sectors represented full time working on mitigation plans.

Ms. RICHARDSON. Okay, so if you could supply to the committee the different levels that you worked with and approximately how many. So, for example, of corporations, if out of the 2,000 you have worked with, 1,500 are major Fortune 500 companies, then say that. If 10 percent are small business, say that.

Mr. MCGURK. Yes, ma'am.

Ms. RICHARDSON. My last question. In the event of a cyberattack, who is in charge?

Mr. MCGURK. In the event of a cyberattack, ma'am, the President is in charge. The President has designated the Secretary of

Homeland Security as the senior Federal official for incident response and incident coordination.

Ms. RICHARDSON. Do you believe that is understood with the Pentagon and NSA and so on?

Mr. MCGURK. I believe that the Pentagon and NSA understand that the President is in charge.

Ms. RICHARDSON. If something were to happen in the private sector, what would be the response?

Mr. MCGURK. The response, in accordance with the National Cyber Incident Response Plan, would be a coordination effort on the part of the Department, working with those private-sector entities or those individual companies to mitigate the risk and prevent it from cascading into other areas.

Ms. RICHARDSON. Thank you very much.

Mr. MCGURK. Thank you, ma'am.

Ms. RICHARDSON. I yield back.

Mr. LUNGREN. Thank you.

The gentleman from Pennsylvania is recognized for 5 minutes.

Mr. MARINO. Thank you, Mr. Chairman.

I have a question for each of you. I have 5 minutes, so we have about a minute and 15 seconds for each, so I will start with Dr. Amoroso.

Can we really stay ahead of the criminals?

Mr. AMOROSO. Well, historically, we haven't, and we probably should assume that we won't. I mean, it makes sense to take a pretty conservative view as we build out our protection approaches. So I think the answer to that is "no."

Mr. MARINO. Because they are going to have the information that—even if the Government puts out there that the citizens are aware of, and they are always trying to manipulate and massage that. So we have to come up with a system whereby we try to step ahead of them, if that is possible.

Mr. AMOROSO. Right.

Mr. MARINO. Attorney Carlin, I am an attorney, too. I was a prosecutor for 18 years. So I know, as the doctor said, once you get some attorneys involved, particularly at the bureaucratic level, it can be a real catastrophe. But what legal issues do you think we face from a liability standpoint if the Government gets involved and, for example, mandates?

Ms. CARLIN. First, I am a reformed lawyer. So I am not actively practicing, but I am in inactive status.

I think there are plenty of legal and policy issues that have not been sorted through, and I think that is part of what we would contemplate, including in this information-sharing protocol or framework exercise, including, quite obviously, privacy issues.

A couple of points, just to add them to your consideration.

One is, when we talk about information sharing, we mean that bilaterally. So there is an equivalent interest on the part of Government in having private industry disclose events as they are happening in our respective companies as there is on the part of private industry in having the Government disclose when they are, frankly, working on something that we may not be aware of.

The emphasis that I have placed on contextual information I think is part of the secret sauce of being more proactive on a going-forward basis. The signatures, the technical information is obviously critical to shutting down that board, that opportunity for malicious behavior. But the context is what allows us to plan for the next attack.

It is not that the same person will do it in the same way, attacking the same server. It is extrapolating from the experience that we have had to contemplate other comparable vulnerabilities and to get ahead in that way by shutting them down.

Mr. MARINO. All right. Thank you.

If you haven't noticed, I am taking advantage of your educational backgrounds. Mr. Cauley, you have an MBA. Does a company or the Government, for that matter, balance the implementation, the cost to the risk before making any decision?

Mr. CAULEY. Thank you for the question. I am really an engineer, but the MBA was incidental.

We really strive to do that both at NERC, as the industry organization, as well as across the industry to assess risk priorities. We deal with hurricanes and other natural disasters as well as these emerging new risks. So it is always a challenge to make the greatest value of the customers', the rate payers' investment in reliability and a reliable supply of electricity.

So I think cost is always a consideration, and I think maximizing value against the risks that we are facing is always something that we are looking at.

Mr. MARINO. Okay. Thank you.

Mr. McGurk, taking advantage of your psychology background, can we really persuade the public in business and, for that matter, as a last resort, the Government to take the steps necessary to effectuating protection against ourselves? What do we need to do to persuade people like myself, not only the computer in my home but the computer in my office and the small business that my wife has?

Mr. MCGURK. Thank you for the question, sir.

I would like to also add on to what Mr. Cauley had said, is that when we are evaluating risk—and in the Department we define risk as threat, vulnerability, and consequence—each of those variables is relevant. Then you need to divide that over cost. So we have to identify where can we get the most benefit or the most gain by addressing the vulnerabilities, the threats, or the consequences.

So making it actionable for the asset owners and operators of the general public and making it understandable, taking all the ones and zeros out and putting it in a language that people can readily understand, helps us convey that message. Getting away from the geek speak and getting into the real speak is what our primary focus is.

Mr. MARINO. Good. Thank you.

I yield.

Mr. LUNGREN. The other gentleman from Pennsylvania, Mr. Meehan, is recognized for 5 minutes.

Mr. MEEHAN. Thank you, Mr. Chairman.

I want to thank the panel for their testimony. I apologize, because of the nature of our work, we aren't always able to be here for the full time. But I did take the time to read each of your written testimonies last night. As a former prosecutor, United States Attorney, I am very interested in these issues.

Let me just ask, stepping back, because, Mr. Amoroso, I was struck by some of your comments. In our effort to try to assure that both the private sector and the Government are working together in this area of assuring cybersecurity, you know, you have some testimony that says the initiatives don't take full advantage of the portfolio of managed services offered by many private-sector network service providers. You were discussing the Federal Government.

Just the panel, in essence, we have the National Infrastructure Protection Plan. It was put in place to pull the Federal Government together with the private sector to use all of our assets to try to do, you know, protect this infrastructure. What should we be doing? Is it working? What is not working?

Mr. Amoroso, I want to ask you specifically because you made this note. If other panelists in my remaining 3 minutes and 40 seconds have observations, I would like to hear from you as well.

Mr. AMOROSO. Well, most of the ideas are great. It is just the technology and infrastructure changes so quickly that it is hard to keep up.

For example, we talk about air gap. My company is in the business of using the air to connect systems. So it is almost—it doesn't make a lot of sense to even talk architecturally about something that made a lot of sense 10 years ago. I spent a lot of time trying to air gap systems in AT&T. We used to have two jacks in the wall; and, depending on what network you were on, you would sort of air gap between this and that.

In 2011, that makes no sense. Equipment comes built in with 3G, 4G connectivity. You have to change all the assumptions.

So the problem is, private sector, you know, through competition and through mobility and cloud and all these exciting things that we use to try to generate interest amongst customers to buy our services, we are moving at a rate that is almost impossible to keep up with from the perspective of kind of the way we legislate and regulate. It takes a long time to debate these issues. By the time you have debated and come to some agreement on something it is largely irrelevant. So we really have to come to a different approach.

Mr. MEEHAN. Well, how do you do that? How do you police that? Because, in essence, you are right. The technology is always going to be ahead. The only thing is that the cyber sleuths are trying to catch up with the technology. That may be that you are one step ahead, but, as Mr. Marino pointed out, there is a lot of people that are still using simplistic systems that are being victimized as well.

Mr. AMOROSO. It is tricky. You have to build forward-looking constructs and then let them work the way you set them up to work without sort of worrying about every little thing. Every day-to-day detail has to be allowed to track technology growth and innovation.

So, you know, the comment I made earlier about signatures, you know, the fact that anytime some information sharing is posed, at least in our company, there is a big debate about each and every situation. I think what we need is a broader framework that allows us a little bit more leeway so that if technology goes in this direction or that direction or whatever, the framework would be broad enough to allow us to be flexible. I think we have been too inflexible in that regard.

Mr. MEEHAN. Thank you.

Ms. Carlin, did you have a thought?

Ms. CARLIN. I just wanted to add one comment. I am not a native technologist, by the way, so maybe it gives me a different perspective.

I don't think it is all about technology and sort of trying to keep apace with the criminal and the nation state elements and such. I think there is a large component that relates to behavior and practices, and I will give you one quick example.

As we have seen in all these incidents, the criminals are increasingly targeting what we might call target-rich environments. You see that in all kinds of respects. You see it at the exchange level. You saw it in the RSA incident. You see it in Epsilon. Why Epsilon? Because it was a warehouse of all of these other connections and such.

So on the practices level, there are many opportunities for improvement, and I will share one with you. We have privileged users—so-called privileged users in our environment who are often IT administrators who have much broader access to data and applications than the average employee would have. We have significantly tightened standards around behavior by IT administrators, how they access the network, how they change their passwords, how frequently, password sharing. I could give you a litany of practices.

So I think let's not put all of our eggs in the—we need the new-age technology. That is part of it.

Mr. MEEHAN. Thank you, Mr. Chairman.

Mr. LUNGREN. Thank you.

I want to thank the witnesses. The reason why we were able to stay here this long is they changed the votes on the floor, and now we have a series of votes. So I thank you for being with us, and we were able to get through the panel and not have to keep you here in suspense.

One of the things I would just ask is that I hope that you would continue to work with us. We don't, obviously, have all the answers. We have got some of the questions. We probably don't have all the questions. Perhaps the overarching question we have is: How do we make it work better? That is, the Government/private-sector partnership. It is a continuing question that is going to bedevil us, but we need to look at it and work with it, and you folks have helped us today. But I hope we could ask you to help us in the future as well.

We thank you very much for your testimony. It has been very, very helpful. There may be some questions offered by some of the Members of the panel in writing to you; and if that is done, we would hope that you would respond to that to help us.

Again, your full statements are made a part of the record.

We thank you for being with us, and this hearing is adjourned.

[Whereupon, at 11:16 a.m., the subcommittee was adjourned.]

○