EXAMINING THE CYBER THREAT TO CRITICAL INFRASTRUCTURE AND THE AMERICAN ECONOMY

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

MARCH 16, 2011

Serial No. 112–11

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

72–221 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*
KERRY ANN WATKINS, *Senior Policy Director*
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

EXAMINING THE CYBER THREAT TO CRITICAL INFRASTRUCTURE AND THE AMERICAN ECONOMY

Wednesday, March 16, 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 10:05 a.m., in Room 311, Cannon House Office Building, Hon. Daniel E. Lungren [Chairman of the subcommittee] presiding.

Present: Representatives Lungren, McCaul, Walberg, Meehan, Long, Marino, Clarke, Richmond, and Keating.

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

The subcommittee is meeting today to hear testimony from Phil Reitinger, the Deputy Under Secretary for National Protection and Programs Directorate of DHS; Gregory Wilshusen, the Director of Information Security Issues at GAO; Phyllis Schneck, Vice President and Chief Technology Officer at McAfee, Inc.; James Lewis, Director and Senior Policy Fellow at the Center for Strategic and International Studies; and Mischel Kwon, President of Mischel Kwon Associates, LLC.

Today we will examine the cyber threat to U.S. critical infrastructure, how it affects the economy, and what Government is doing to address the threat.

Twenty-five years ago, the concept of cyber threat, or a cyber attack, was an issue of interest to really only a few researchers in academics. In this post-9/11 terrorist era the cyber threat is serious, multifaceted, and boundless, posing a significant risk to U.S. economic and National security.

The Director of National Intelligence stated in testimony before the Congress, "The growing connectivity between information systems, the internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, financial networks, and other critical infrastructures."

The information revolution launched by the internet has reached into every corner of our lives. While it provides users many benefits, it also exposes them to new and dangerous risks. These new risks include cyber criminals, spies and terrorists, using the digital

internet as a pathway to personal bank accounts as well as Government and industrial secrets. Cyber attacks are growing more frequent, targeted, sophisticated, and dangerous.

Most of these attacks are motivated by financial or intellectual property theft, disruption of commerce, or intelligence collection. Cyber attacks have been launched against nations, Estonia in 2007, Georgia in 2009, and Iran in 2010. They were all the subject of cyber attacks that either paralyzed Government operations or targeted critical infrastructure. Last year, Google and 20 other major companies were the targets of highly sophisticated attacks to steal their intellectual property and user accounts. This attack allegedly emanated from China.

If terror groups are watching this cyber activity and targeting our critical infrastructure—and we believe they are—this raises the stakes in our war on terror. U.S. critical infrastructure—by that I mean roads, bridges, dams, electrical system, power systems—overall, that critical infrastructure is the backbone of our dynamic and productive economy. Attacks on this critical infrastructure will impact our National and economic security as well as the health and safety of our fellow citizens.

Today, our critical infrastructure relies extensively on computerized information systems and the internet which cannot be protected as in the traditional way with guns, gates, and guards. This reliance on computers and the internet makes our critical infrastructure operations vulnerable to cyber attack. This vulnerability was demonstrated a few years ago in a simulated attack on our electric power grid, which also was code-named Aurora.

The computer security company, McAfee, reports that 54 percent of executives of critical infrastructure companies surveyed said their companies had been the victims of denial of service attacks and network infiltration from organized crime, terrorists, or other nation states.

Recent media reports have described a new cyber threat called Stuxnet, which can target critical infrastructure, including nuclear facilities. According to these published reports, Stuxnet is a complex piece of malware designed to interfere with the seamen's industrial control systems operating the Iranian nuclear facilities. This makes Stuxnet, at least according to published reports, it makes that malware a very dangerous offensive cyber weapon that overtakes critical control system operations.

So if an anonymous enemy or terrorist ever seizes the control systems of, let's say, dams or chemical or power plants via the cyber world, that terrorist could cause death and destruction in the real world.

So many questions remain about how to defend our cyberspace. What solutions, policies, or technology can we develop to improve our Nation's cybersecurity? We welcome our public and private witnesses today who will begin us on a journey to answer these questions.

It is now my pleasure to recognize the Ranking Member of our subcommittee, Ms. Clarke, for her opening statement.

Ms. CLARKE. Good morning, and thank you to all of our witnesses for appearing before us today.

I would like to thank Chairman Lungren for holding this hearing on cybersecurity and for your intention to move expeditiously on what I know we both recognize as a critical issue.

While there are a number of new faces up here on the dais, I believe this subcommittee will continue to place significant focus on the issue of cybersecurity just as we did during the 110th Congress. I know Mr. Lungren takes this responsibility as seriously as I do, and I look forward to partnering with him again over the next 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 likely be the first of several cybersecurity hearings that the subcommittee will hold, and it is easy to understand why this issue dominates our agenda. We rely on information technology in every aspect of our lives, from our electric grid, banking systems, military and government functions, to our e-mail and web browsers. 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 stopped to consider the security ramifications of this new world we were creating, and so we find ourselves in an extremely dangerous situation today.

Too many vulnerabilities exist on too many critical networks which are exposed to too many skilled attackers who can inflict too many intrusions into 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 sound the alarm, raise awareness of the problems we face, and move forward with practical, effective solutions.

This hearing comes at a critical moment in our Nation's approach to the cyber threat. 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.

We are expecting, and this committee is eager to see, a National cybersecurity strategy from the White House to be released very soon. The Department is finalizing its National cyber incident response plan and will also include a cybersecurity strategy as called for in the 2010 Quadrennial Homeland Security Review.

The Congress is interested in legislation to afford DHS authority it needs to protect the dot-gov domain and critical infrastructures in the private sector. The previous two decades have seen countless reports from America's thought leaders in cybersecurity containing hundreds of recommendations about how to improve America's posture in cyberspace. What has been lacking is the courage and leadership to actually implement these recommendations. To ensure our National and economic security, now is the time we must act.

The U.S. Government must chart a new course to cyberspace. The private sector must also be a full partner and accept its share of responsibility for our combined security. Now is the time to stop planning and start acting.

The Chairman's intention with this hearing is to give this subcommittee some background on the issues facing us. Cybercrime

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. The enemy has already successfully attacked and continues to do so. We need to absorb this information, get up to speed quickly, and move forward to address this issue. We have already lost many small battles. 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. 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.

Thank you, Chairman, and I yield back.

Mr. LUNGREN. Thank you very much, Madam Ranking Member, and I appreciate your spirit of cooperation with which you led this subcommittee and continuing now.

Other Members are reminded that they may give us their statements that will be entered into the record.

We are pleased to have a very distinguished panel of witnesses before us today on this important topic. Deputy Under Secretary Phil Reitinger was named Deputy Under Secretary for NPPD in 2009. He also serves as the Director of the National Cybersecurity Center. In this role, he provides strategic direction to the Department's cybersecurity efforts. Prior to joining the Department, he was the senior security strategist for Microsoft's trustworthy computing program, so he is well versed in the challenges facing both Government and the private sector in dealing with the important issue of cybersecurity.

Prior to serving with Microsoft, Deputy Under Secretary Reitinger was the Executive Director for the Department of Defense's Cybercrime Center. Before that, he was the Deputy Chief of the Department of Justice's Computer Crime and Intellectual Property Section, proving that he just can't keep a job. No. He has had tremendous experience and has a unique perspective from multiple positions within the administration and therefore has much wisdom with which to guide us.

Greg Wilshusen has been with the GAO for over 13 years and has been over 29 years in auditing financial management information systems. He is a certified public accountant, certified internal auditor, certified information systems auditor. He holds a B.S. degree in business administration from the University of Missouri. Are they in the——

Mr. WILSHUSEN. Yes, they are. In fact, they are playing tomorrow evening at 9:50 against——

Mr. LUNGREN. I see. Notre Dame doesn't play until Friday at 1:40 eastern time, but I hope to be in California so I will be watching them from the Pacific coast.

An MS in information management from George Washington University School of Engineering and Applied Sciences. At GAO, he

has overseen multiple reports on information security, both at DHS and Government-wide.

The Chair recognizes Mr. Reitinger, who will testify on behalf of the Department of Homeland Security.

STATEMENT OF PHILIP REITINGER, DEPUTY UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Mr. REITINGER. Thank you very much, Chairman Lungren and Ranking Member Clarke. It is indeed an honor to be here today to talk before the committee.

As you pointed out, sir, my name is Phillip Reitinger, and I am the Deputy Under Secretary at the Department of Homeland Security.

Appropos of your comment about my inability to keep a job, I would say I am not sure I need to be here today based on the opening comments that you and the Ranking Member made. Let me give you an Amen from the congregation; you understand the issue, you get it. So I am going to speak very briefly about three quick points, and then I would be happy, after Greg talks, to answer any questions that you have.

The three points I wanted to quickly raise are that cybersecurity is a critical issue; second, there is no simple solution, neither entity or technology, that is going to solve the problem; and three, that although we have made significant progress over the course of my 15 to 20 years involved in this space and the more significant efforts of many more people over a longer period of time, we are not yet where we need to be. We need to actually—not to be jargonistic, but we need to take this to a new level.

So let me start with the first point, that cybersecurity is a critical issue. This goes back to the comments that you made, Chairman. The threat is significant, and the threat is getting more significant. Perhaps more important, we are depending more on information networks every day—not just for looking at a cute video online or our ability to send an e-mail, but for the basic functioning of our economy.

It is not just a security issue, it is an economic issue. We don't have power, we don't have phone service, we don't have 9–1–1 service, we don't get water, we don't have banking without the proper functioning of the internet and the systems that are connected to it. So we must treat this as a critical issue, and, in fact, we have, over the course of the last two administrations. Cybersecurity has been a bipartisan issue, going from the launch of the Comprehensive National Cybersecurity Initiative in the prior administration through the current Presidents's Cyberspace Policy Review and the on-going work to cross both administrations and across both parties in both Houses of Congress to move the issue forward.

But it is a complex problem. There is no simple solution. There is no single entity, no private sector player or even the private sector together. DHS, DOD, the Department of Commerce, all of them need to be involved, and none of them standing alone—and none of them even standing in the forefront with a little bit of help from others is going to solve the problem. We actually do have to work this broadly in partnership. By partnership, I don't mean saying

partnership we all sing Kumbaya and we go home. I mean, we actually work together to drive outcomes, that we have known roles and responsibilities and we execute on those things.

In that space, DHS plays a critical role. We are responsible for leading the protection of the civilian government systems and private sector, so-called dot-com systems, even though it is broader than that. I say "lead" advisedly because this is not about DHS will come in and solve all your problems for you. We are not going to do that. But what we can do is we can help. Everybody has got to build security into their own operations—private sector companies, civilian government agencies and DHS; we have got to build it into our DNA. DHS has got to do the job of helping people to execute much more effectively. We have had signal successes in that role. The Chairman mentioned the creation of the first real National incident response plan to bring all of Government and private sector together so we can respond as one Nation to a significant cyber event.

A plan that we tested in a major exercise last year that involved several thousand people—literally, several thousand people around the globe, tens of private sector companies, over 10 nations around the world and over 10 States and localities. I will talk more after my opening statement in response to your questions.

The last thing I would say in closing is that much more remains to be done. As the Ranking Member indicated, we are systemically vulnerable. We have made significant progress, but we are not yet where we need to be. So as the Ranking Member indicated, what we have to do is focus on implementation. What makes a difference day to day, week to week, month to month? How can we do that? That is one of the reasons why partnership from the Government Accountability Office is so important to us. It can help us prioritize, indicate areas for further progress, and help us find the best way forward.

Together, we need to have that broad public dialogue which I am sure will take place this year across the public and private sectors about how we close the gap between where we are now and where we need to be. With that, I will look forward very much to the questions of the subcommittee. Thank you.

[The statement of Mr. Reitinger follows:]

PREPARED STATEMENT OF PHILIP REITINGER

MARCH 16, 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. I will provide an overview of the current cybersecurity environment, the Department's cybersecurity mission as it relates to critical infrastructure, and the coordination of this mission with our public and private sector partners.

We would like to work more with you to convey the relevance of cybersecurity to average Americans. Increasingly, the services we rely on for 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 confronts 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 information collection and sharing process, and as bad as the loss of precious National intellectual capital is, we increasingly face threats that are even greater. We currently cannot be certain that our information infrastructure will remain accessible and reliable during a time of crisis.

We face persistent, unauthorized, and often unattributed intrusions into Federal Executive Branch civilian networks. These intruders span a spectrum of malicious actors, including nation states, terrorist networks, organized criminal groups, or individuals located here in the United States. They 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, dismantle, 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, and confidence in Government. 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. Moreover, securing cyberspace is also critical to accomplishing nearly all of DHS's other missions successfully.

We need to support the efforts of our State and local government and private sector partners to secure themselves against malicious activity in cyberspace. Similarly, we need to ensure that the Federal civilian environment is secure and that legitimate traffic is allowed to flow freely while malicious traffic is prevented from penetrating our defenses. Collaboratively, public and private sector partners must use our knowledge of these 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. In addition, other departments, such as the Department of Education, are working to educate parents and students on internet safety and privacy protection.

CYBERSECURITY MISSION

Let me be clear that no single technology—or single Government entity—alone can overcome the cybersecurity challenges our Nation faces. Cybersecurity must start with informed users taking necessary precautions and extend through a coordinated effort between the private sector, critical infrastructure owners and operators, and the extensive expertise that lies across coordinated Government entities. The National Protection and Programs Directorate (NPPD) within DHS is responsible for the following key cybersecurity missions:

- Leading the effort to secure Federal Executive Branch civilian departments and agencies' unclassified networks;
- 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.
- Leveraging cyber defense capability across all departments and agencies to detect, respond, isolate, and remediate cyber attacks or practices dangerous to security and privacy.

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 evolve to become 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 Nation's 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. 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 proactively 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. Simply put, the cybersecurity mission cannot be accomplished by any one agency; it requires teamwork and coordination. Together, we can leverage resources, personnel, and skill sets that are needed to achieve a more secure and reliable cyberspace.

NCSD collaborates with Federal Government stakeholders, including civilian agencies, law enforcement, the military, the intelligence community, State and local partners, and private sector stakeholders, to conduct risk assessments and mitigate vulnerabilities and threats to information technology assets and activities affecting the operation of civilian government and private sector critical infrastructures. NCSD also provides cyber threat and vulnerability analysis, early warning, and incident response assistance for public and 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. The plan 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 National Cyber Incident Response Plan 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 National Cybersecurity and Communications Integration Center (NCCIC)—DHS' 24-hour cyber watch and warning center—and the Federal Government's full suite of cybersecurity response capabilities. 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 (NCC), are collocated into 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 are located at the NCCIC. We are also finalizing steps to add representatives from the Banking and Finance sector, as well as the Multi-State Information Sharing and Analysis Center (MS–ISAC).

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 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.

PROVIDING TECHNICAL EXPERTISE TO THE PRIVATE SECTOR AND CRITICAL INFRASTRUCTURE

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 shown 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 them 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 computer network defense and protection rather than law enforcement or intelligence functions. DHS engages precisely to mitigate the threat to the network to reduce future risks.

Our approach requires vigilance and a voluntary public-private partnership. Indeed, we are continuing to build our capabilities and our relationships; we must because the cyber threat trends only more sophisticated and more frequent.

Over the past year, we stood up 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 are increasing training available to our employees. We have an operational National Cyber Incident Response Plan (NCIRP), and we continue to update and improve it with input from senior cybersecurity leaders. We will be releasing the NCIRP publicly in the coming weeks. 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.

US–CERT provides remote and on-site response support and defense against malicious cyber activity for the Federal Executive Branch civilian networks. US–CERT also collaborates, provides remote and on-site response support and shares information with State and local government, critical infrastructure owners and operators, and international partners to address cyber threats and develop effective security responses.

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 depend on the energy sector, and failure in one of these sectors could subsequently affect Government and private sector operations.

NCCIC'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 (SCADA), 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.

ICS–CERT provides on-site support to owners and operators of critical infrastructure for protection against and response to cyber threats, including incident response, forensic analysis, and site assessments. ICS–CERT also provides tools and training to increase stakeholder awareness of evolving threats to industrial control systems.

A 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, we attempt to balance the need for public information sharing while limiting 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 in-

stallations 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.

PROTECTING FEDERAL CIVILIAN GOVERNMENT NETWORKS

In addition to its support of private sector owners and operators of infrastructure, DHS also collaborates with its partners to increase the security of Federal Executive Branch civilian agency networks. The fundamental ways that DHS works to secure Federal networks are by improving the ability of departments and agencies to defend their systems and by directly providing expertise and specific technology that detects, mitigates, and prevents malicious activity on these networks.

As part of the CNCI, DHS works with the Office of Management and Budget (OMB) to reduce and consolidate the number of external connections that Federal agencies have to the internet through the Trusted Internet Connection (TIC) initiative. This initiative reduces the number of entry points for potential vulnerabilities into Government networks and allows DHS to focus monitoring efforts on limited and known avenues through which internet traffic must travel. DHS conducts onsite evaluations of agencies' progress toward implementing TIC goals.

In conjunction with the TIC initiative, the EINSTEIN system is designed to provide the U.S. Government with an early warning system for intrusions to Federal Executive Branch civilian networks, near real-time identification of malicious activity, and automated disruption of that malicious activity. The second phase of EINSTEIN, known as EINSTEIN 2 and developed in 2008 as part of the CNCI, incorporates intrusion detection capabilities into the original EINSTEIN system. DHS is currently deploying EINSTEIN 2 to Federal Executive Branch civilian agency TIC locations and Networx Managed Trusted Internet Protocol Services (MTIPS) providers, which are private internet service providers that serve Federal agencies, to assist them with protecting their computers, networks, and information. EINSTEIN 2 has now been deployed at 15 of the 19 large departments and agencies who maintain their own TIC locations. Also, the four MTIPS providers currently provide service to seven additional Federal agencies. In 2010, EINSTEIN 2 sensors registered 5.4 million "hits," an average of more than 450,000 hits per month or nearly 15,000 hits per day. A hit is an alert triggered by a predetermined intrusion detection signature that corresponds to a known threat. Each hit represents potential malicious activity for further assessment by US–CERT.

DHS is currently developing the third phase of the EINSTEIN system—an intrusion prevention capability which will provide DHS with the ability to automatically detect and disrupt malicious activity before harm is done to critical networks and systems. In advance of this development, DHS, in coordination with the National Security Agency (NSA), conducted the CNCI Initiative 3 Exercise, which advanced the potential capabilities of the EINSTEIN system by demonstrating defensive technology, sharing near real-time threat information with DoD for enhanced situational awareness, and providing a platform upon which an oversight and compliance process can be implemented for the evolving set of EINSTEIN capabilities. The Department's Privacy Office and its Office for Civil Rights and Civil Liberties carefully reviewed the exercise concept of operations, and the Privacy Office worked with US–CERT to publicly release a detailed Privacy Impact Assessment evaluating the exercise. US–CERT also briefed the exercise to the cyber subcommittee of the independent DHS Data Privacy and Integrity Committee.

Beyond the TIC initiative and the EINSTEIN system, DHS, OMB, and the National Institute for Standards and Technology work cooperatively with agencies across the Federal Government to coordinate the protection of the Nation's Federal information systems through compliance with the Federal Information Security Management Act of 2002 (FISMA). US–CERT monitors EINSTEIN 2 sensors for intrusion activity and receives self-reported incident information from Federal agencies. This information is reported to OMB for use in its FISMA oversight capacity. In 2010, DHS also began to administer oversight of the CyberScope system, which was developed by the Department of Justice. This system collects agency information regarding FISMA compliance and, as DHS, OMB, and their agency partners move toward automated reporting, the system will enable real-time assessments of baseline security postures across individual agencies and the Federal enterprise as a whole. This activity complements the development of reference architectures that

DHS designs for Federal agency stakeholders that are interested in implementing security solutions based on standards and best practices. DHS also works with the General Services Administration to create Blanket Purchase Agreements that address various security solutions for Federal agencies.

THE DHS CYBERSECURITY WORKFORCE

As DHS continues to make progress on initiatives such as TIC and EINSTEIN, the Department is also mindful that the Nation's cybersecurity challenge will not be solved by a single technology solution. Multiple innovative technical tools are necessary and indeed, technology alone is insufficient. The mission requires a larger cybersecurity professional workforce, governance structures for enhanced partnerships, more robust information sharing and identity protection, and increased cybersecurity awareness among the general public. Responsibility for these solutions is, and will remain, distributed across public and private sector partners.

DHS is focused on building a world-class cybersecurity team by hiring a diverse group of cybersecurity professionals—computer engineers, scientists, and analysts—to secure the Nation's digital assets and protect against cyber threats to our critical infrastructure and key resources. NCSD continues to hire cybersecurity and information technology professionals, nearly tripling its cybersecurity workforce in fiscal year 2009 and nearly doubling that number again in fiscal year 2010. NCSD currently has more than 230 cybersecurity professionals on board, with dozens more in the hiring pipeline.

Several initiatives are designed to increase the Nation's number of highly qualified cybersecurity professionals. DHS and NSA co-sponsor the Centers of Academic Excellence in Information Assurance Education and Research programs, the goal of which is to produce a growing number of professionals with information assurance expertise in various disciplines. DHS and the Department of State co-hosted Operation Cyber Threat (OCT1.0), the first in a series of Government-wide experiential and interactive cybersecurity training pilots designed to apply learning concepts and share best practices in a secure, simulated environment to build capacity within the Federal workforce. In December 2010, the Institute of Electrical and Electronics Engineers Computer Society, the world's leading organization of computing professionals, formally recognized the Master of Software Assurance (MSwA) Reference Curriculum, which DHS sponsored through its Software Assurance (SwA) Curriculum Project. The MSwA program is the first curriculum of its kind to focus on assuring the functionality, dependability, and security of software and systems. Finally, DHS co-sponsored the annual Colloquium for Information Systems Security Education and the Scholarship for Services (SFS) Job Fair/Symposium, which brought together 55 Federal agencies and more than 200 SFS students.

The National Initiative for Cybersecurity Education (NICE) has the dual goals of a cyber-savvy citizenry and a cyber-capable workforce. Working with NIST, which is the overall interagency lead, DHS heads the NICE awareness elements and co-leads the training and professional development components with DoD and the Office of the Director of National Intelligence.

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 controls cyberspace and the success of our cybersecurity mission relies on effective communication and critical partnerships. Many Government players have complementary roles—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.

DHS works closely with its Federal, State, and local partners to protect Government cyber networks. In September 2010, DHS and DoD signed a memorandum of agreement that aligns and enhances America's capabilities to protect against threats to our critical civilian and military computer systems and networks, including deploying a National Security Agency support team to the NCCIC to enhance the National Cyber Incident Response Plan and sending a full-time senior DHS leader and support team to the National Security Agency.

In November 2010, the MS–ISAC opened its Cyber Security Operations Center, a 24-hour watch and warning facility, which will both enhance situational awareness at the State and local level for the NCCIC and allow the Federal Government to quickly and efficiently provide critical cyber risk, vulnerability, and mitigation data to State and local governments. An MS–ISAC analyst/liaison is collocated in the NCCIC.

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. Within current legal authorities, DHS engages with the private sector on a voluntary basis. 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 local 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. This fulfills 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 December 2010, DHS 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.

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, seven 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.,* a message developed with the private sector, 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 (NICE).

Throughout its public and private sector activities, DHS is committed to supporting 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 collaboration across the homeland security enterprise. The Department of Homeland Security 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. It is important to recognize that we do not undertake cybersecurity for the sake of security itself, but rather to ensure that Government, business, and critical societal functions can continue to use the information technology and communications infrastructure on which they depend.

Within our current legal authorities, DHS continues to engage and collaborate with partners in the private and public sectors. We are deploying intrusion detection and prevention technologies across the Federal enterprise, aiding departments and agencies in securing their networks, and providing analysis, vulnerability, and mitigation assistance to private sector CIKR partners. Our continued dedication to privacy, 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 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 end 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. Reitinger.

Now Mr. Wilshusen, who is looking forward to tomorrow's basketball game, if you could give us about 5 minutes of your best pitch right now and then we can ask questions.

STATEMENT OF GREGORY WILSHUSEN, DIRECTOR OF INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Chairman Lungren, Ranking Member Clarke, and Members of the subcommittee, thank you for the opportunity to testify at today's hearing on cyber threats to critical infrastructure and the American economy.

As you mentioned in your opening statements, pervasive and sustained cyber attacks against the United States continue to threaten Federal and non-Federal systems and operations. The every-increasing interdependence on these systems to carry out essential everyday operations and activities makes us vulnerable to a wide array of cyber-based threats. Thus, it is increasingly important that Federal and non-Federal entities carry out concerted efforts to safeguard their systems and the information they contain.

Mr. Chairman, today we will discuss the threats to cyber-reliant critical infrastructures and with Federal information systems and the challenges agencies face in protecting them.

Cyber threats to critical infrastructure and Federal services are evolving and growing and can come from a variety of sources, including criminals and foreign nations, as well as hackers and disgruntled employees. It is important not to forget about the insider threat. Potential hackers have a variety of techniques at their disposal that can vastly expand the risk, the reach, and impact of their operations, including use of social engineering and malicious software. The interconnectivity between information systems, the internet, and other infrastructure also presents increasing opportunities for such attacks. Not surprisingly, security incidents reported by Federal agencies are on the rise, increasing over 650 percent during the past 5 years to nearly 42,000 in fiscal year 2010.

Cyber attack incidents can seriously impact our National and economic security and have resulted in the loss of classified information and intellectual property, and financial crimes reportedly totaling billions of dollars. Although the administration and Federal agencies continue to act to strengthen the Nation's cybersecurity posture, challenges remain. Key actions to improve our National approach to cybersecurity have not been fully implemented, Federal capacity to protect against cyber threats needs to improve, and Federal agencies have not fully addressed persistent control weaknesses or consistently implemented effective information security programs. For these reasons, GAO once again identified protecting the Federal Government's information systems and the Nation's critical infrastructure as a Government-wide high-risk area in its biennial report to the Congress on high-risk Government programs.

Mr. Chairman, much work remains to be done. Additional Federal efforts are needed to implement actions recommended by the President's Cybersecurity Policy Review, update the National strategy for securing the information and communications infrastructure, develop a National strategy for addressing the global aspects of cybersecurity, and create a prioritized National and Federal cybersecurity research and development agenda.

Federal agencies, and in particular DHS, need to enhance their cyber analysis and warning capabilities and help strengthen the effectiveness of public-private sector partnerships in securing cyber critical infrastructure. Federal agencies also need to mitigate known vulnerabilities, fully implement comprehensive information security programs, and facilitate Government-wide efforts to secure their systems.

GAO has made numerous recommendations to assist agencies in these areas, and agencies have implemented or are in the process of implementing many of them.

In summary, Mr. Chairman, the threats to information systems are evolving and growing, and systems supporting Federal operations and the Nation's critical infrastructures are not sufficiently protected to consistently thwart those threats. Until the administration and Federal agencies working with the private sector fully address the challenges before them, our Nation's cybersecurity critical infrastructure will remain vulnerable.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions.

[The statement of Mr. Wilshusen follows:]

PREPARED STATEMENT OF GREGORY WILSHUSEN

MARCH 16, 2011

CYBERSECURITY: CONTINUED ATTENTION NEEDED TO PROTECT OUR NATION'S CRITICAL INFRASTRUCTURE AND FEDERAL INFORMATION SYSTEMS

Chairman Lungren, Ranking Member Clarke, and Members of the subcommittee: Thank you for the opportunity to testify at today's hearing on the cyber threats to critical infrastructure and the American economy.

Pervasive and sustained cyber attacks against the United States continue to pose a potentially devastating impact on Federal and non-Federal systems and operations. In February 2011, the Director of National Intelligence testified that, in the past year, there had been a dramatic increase in malicious cyber activity targeting U.S. computers and networks, including a more than tripling of the volume of malicious software since 2009.[1] Recent press reports that computer hackers broke into and stole proprietary information worth millions of dollars from the networks of six U.S. and European energy companies also demonstrate the risk that our Nation faces. Such attacks highlight the importance of developing a concerted response to safeguard Federal and non-Federal information systems.

Mr. Chairman, GAO recently issued its high-risk list of Government programs that have greater vulnerability to fraud, waste, abuse, and mismanagement or need transformation to address economy, efficiency, or effectiveness challenges.[2] Once again, we identified protecting the Federal Government's information systems and the Nation's cyber critical infrastructure as a Government-wide high-risk area. We have designated Federal information security as a high-risk area since 1997; in 2003, we expanded this high-risk area to include protecting systems supporting our Nation's critical infrastructure, referred to as cyber critical infrastructure protection or cyber CIP.

In my testimony today I will describe: (1) Cyber threats to cyber-reliant critical infrastructures and Federal information systems and (2) the continuing challenges Federal agencies face in protecting the Nation's cyber-reliant critical infrastructures and Federal systems. In preparing this statement in March 2011, we relied on our previous work in these areas (please see the related GAO products page at the end of this statement). These products contain detailed overviews of the scope and methodology we used. The work on which this statement is based was performed in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

BACKGROUND

As computer technology has advanced, Federal agencies and our Nation's critical infrastructures[3]—such as power distribution, water supply, telecommunications, and emergency services—have become increasingly dependent on computerized information systems to carry out their operations and to process, maintain, and report essential information. Public and private organizations rely on computer systems to transfer increasing amounts of money and sensitive and proprietary information, conduct operations, and deliver services to constituents.

The security of these systems and data is essential to protecting National and economic security, and public health and safety. Conversely, ineffective information security controls can result in significant risks, including the loss of resources, such as Federal payments and collections; inappropriate access to sensitive information, such as National security information, personal information on taxpayers, or propri-

[1] Director of National Intelligence, *Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community,* statement before the Senate Select Committee on Intelligence (Feb. 16, 2011).

[2] GAO, *High-Risk Series: An Update,* (Washington, DC: February 2011).

[3] Critical infrastructures are systems and assets, whether physical or virtual, so vital to the Nation that their incapacity or destruction would have a debilitating impact on National security, National economic security, National public health or safety, or any combination of those matters.

etary business information; disruption of critical operations supporting critical infrastructure, National defense, or emergency services; and undermining of agency missions due to embarrassing incidents that diminish public confidence in Government.

CYBER-RELIANT CRITICAL INFRASTRUCTURE AND FEDERAL SYSTEMS FACE INCREASING CYBER THREATS

Threats to systems supporting critical infrastructure and Federal information systems are evolving and growing. Government officials are concerned about attacks from individuals and groups with malicious intent, such as criminals, terrorists, and foreign nations. Federal law enforcement and intelligence agencies have identified multiple sources of threats to our Nation's critical information systems, including foreign nations engaged in espionage and information warfare, criminals, hackers, virus writers, and disgruntled employees and contractors. These groups and individuals have a variety of attack techniques at their disposal that can be used to determine vulnerabilities and gain entry into targeted systems. For example, phishing involves the creation and use of fake e-mails and websites to deceive internet users into disclosing their personal data and other sensitive information.

The connectivity between information systems, the internet, and other infrastructures also creates opportunities for attackers to disrupt telecommunications, electrical power, and other critical services. For example, in May 2008, we reported that the Tennessee Valley Authority's (TVA) corporate network contained security weaknesses that could lead to the disruption of control systems networks and devices connected to that network.[4] We made 19 recommendations to improve the implementation of information security program activities for the control systems governing TVA's critical infrastructures and 73 recommendations to address weaknesses in information security controls. TVA concurred with the recommendations and has taken steps to implement them. As Government, private sector, and personal activities continue to move to networked operations, the threat will continue to grow.

Reported Security Incidents Are on the Rise

Consistent with the evolving and growing nature of the threats to Federal systems, agencies are reporting an increasing number of security incidents. These incidents put sensitive information at risk. Personally identifiable information about U.S. citizens has been lost, stolen, or improperly disclosed, thereby potentially exposing those individuals to loss of privacy, identity theft, and financial crimes. Agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices. Further, reported attacks and unintentional incidents involving critical infrastructure systems demonstrate that a serious attack could be devastating.

When incidents occur, agencies are to notify the Federal information security incident center—the United States Computer Emergency Readiness Team (US–CERT). Over the past 5 years, the number of incidents reported by Federal agencies to US–CERT has increased dramatically, from 5,503 incidents reported in fiscal year 2006 to about 41,776 incidents in fiscal year 2010 (a more than 650 percent increase). The three most prevalent types of incidents and events reported to US–CERT during fiscal year 2010 were: (1) Malicious code (software that infects an operating system or application), (2) improper usage (a violation of acceptable computing use policies), and (3) unauthorized access (where an individual gains logical or physical access to a system without permission). Additionally, according to Department of Homeland Security (DHS) officials, US–CERT detects incidents and events through its intrusion detection system, supplemented by agency reports, for investigation (unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review).

Reports of cyber attacks and information security incidents against Federal systems and systems supporting critical infrastructure illustrate the effect that such incidents could have on National and economic security.

- In July 2010, the Department of Defense (DOD) launched an investigation to identify how thousands of classified military documents (including Afghanistan and Iraq war operations, as well as field reports on Pakistan) were obtained by the group WikiLeaks.org. According to DOD, this investigation was related to an on-going investigation of an Army private charged with, among other things, transmitting National defense information to an unauthorized source.

[4] GAO, *Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks,* (Washington, DC: May 21, 2008).

- In 2010, the Deputy Secretary of Defense stated that DOD suffered a significant compromise of its classified military computer networks in 2008. It began when a flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network and spread on both classified and unclassified systems.[5]
- In February 2011, media reports stated that computer hackers broke into and stole proprietary information worth millions of dollars from the networks of six U.S. and European energy companies.

THE FEDERAL GOVERNMENT HAS TAKEN ACTIONS TO ADDRESS CYBER THREATS, BUT CHALLENGES REMAIN IN PROTECTING CRITICAL SYSTEMS

The Federal Government has a variety of roles and responsibilities in protecting the Nation's cyber-reliant critical infrastructure, enhancing the Nation's overall cybersecurity posture, and ensuring the security of Federal systems and the information they contain. In light of the pervasive and increasing threats to critical systems, the Executive branch is taking a number of steps to strengthen the Nation's approach to cybersecurity. For example, in its role as the focal point for Federal efforts to protect the Nation's cyber critical infrastructures,[6] DHS issued a revised National infrastructure protection plan in 2009 and an interim National cyber incident response plan in 2010. Executive branch agencies have also made progress instituting several Government-wide initiatives that are aimed at bolstering aspects of Federal cybersecurity, such as reducing the number of Federal access points to the internet, establishing security configurations for desktop computers, and enhancing situational awareness of cyber events. Despite these efforts, the Federal Government continues to face significant challenges in protecting the Nation's cyber-reliant critical infrastructure and Federal information systems.

Key Actions to Improve Our Current National Approach to Cybersecurity Have Not Yet Been Fully Implemented

The administration and Executive branch agencies have not yet fully implemented key actions that are intended to address threats and improve the current U.S. approach to cybersecurity.

- *Implementing actions recommended by the President's Cybersecurity Policy Review.* In February 2009, the President initiated a review of the Government's cybersecurity policies and structures, which resulted in 24 near- and mid-term recommendations to address organizational and policy changes to improve the current U.S. approach to cybersecurity.[7] In October 2010, we reported that 2 recommendations had been implemented and 22 were partially implemented.[8] Officials from key agencies involved in these efforts (e.g., DHS, DOD, and the Office of Management and Budget (OMB)) stated that progress had been slower than expected because agencies lacked assigned roles and responsibilities and because several of the mid-term recommendations would require action over multiple years. We recommended that the National Cybersecurity Coordinator (whose role was established as a result of the policy review) designate roles and responsibilities for each recommendation and develop milestones and plans, including measures to show agencies' progress and performance.
- *Updating the National strategy for securing the information and communications infrastructure.* In March 2009, we testified on the needed improvements to the Nation's cybersecurity strategy.[9] In preparation for that testimony, we convened a panel of experts that included former Federal officials, academics, and private sector executives. The panel highlighted 12 key improvements that are, in its view, essential to improving the strategy and our National cybersecurity posture, including the development of a National strategy that clearly articulates strategic objectives, goals, and priorities.
- *Developing a comprehensive National strategy for addressing global cybersecurity and governance.* In July 2010, we reported that the U.S. Government faced a number of challenges in formulating and implementing a coherent approach

[5] Foreign Affairs, *Defending a New Domain: The Pentagon's Cyberstrategy,* William J. Lynn III, U.S. Deputy Secretary of Defense (New York, NY: September/October 2010).

[6] As established by Federal law and policy, including the Homeland Security Act of 2002, Homeland Security Presidential Directive—7, and the *National Strategy to Secure Cyberspace.*

[7] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: May 29, 2009).

[8] GAO, *Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed,* GAO–11–24 (Washington, DC: Oct. 6, 2010).

[9] GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture,* GAO–09–432T (Washington, DC: Mar. 10, 2009).

to global aspects of cyberspace, including, among other things, providing top-level leadership and developing a comprehensive strategy.[10] Specifically, we found that the National Cybersecurity Coordinator's authority and capacity to effectively coordinate and forge a coherent National approach to cybersecurity were still under development. In addition, the U.S. Government had not documented a clear vision of how the international efforts of Federal entities, taken together, support overarching National goals. We recommended that, among other things, the National Cybersecurity Coordinator develop with other relevant entities a comprehensive U.S. global cyberspace strategy. The coordinator and his staff concurred with our recommendations and stated that actions had already been initiated to address them.

- *Finalizing cybersecurity guidelines and monitoring compliance related to electricity grid modernization.* In January 2011, we reported on efforts by the National Institute of Standards and Technology (NIST) to develop cybersecurity guidelines and Federal Energy Regulatory Commission (FERC) efforts to adopt and monitor cybersecurity standards related to the electric industry's incorporation of IT systems to improve reliability and efficiency—commonly referred to as the smart grid.[11] We determined that NIST had not addressed all key elements of cybersecurity in its initial guidelines or finalized plans for doing so. We also determined that FERC had not developed an approach for monitoring industry compliance with its initial set of voluntary standards. Further, we identified six key challenges with respect to securing smart grid systems, including a lack of security features being built into certain smart grid systems and an ineffective mechanism for sharing information on cybersecurity within the industry. We recommended that NIST finalize its plans for updating its cybersecurity guidelines to incorporate missing elements and that FERC develop a coordinated approach to monitor voluntary standards and address any gaps in compliance. Both agencies agreed with these recommendations.
- *Creating a prioritized National and Federal cybersecurity research and development (R&D) agenda.* In June 2010, we reported that while efforts to improve cybersecurity R&D were under way by the White House's Office Science and Technology Policy (OSTP) and other Federal entities, six major challenges impeded these efforts.[12] Among the most critical was the lack of a prioritized National cybersecurity research and development agenda. We found that despite its legal responsibility and our past recommendations, a key OSTP subcommittee had not created a prioritized National R&D agenda, increasing the risk that research pursued by individual organizations will not reflect National priorities. We recommended that OSTP direct the subcommittee to take several actions, including developing a National cybersecurity R&D agenda. OSTP agreed with our recommendation and provided details on planned actions.

We are in the process of verifying actions taken to implement our recommendations. In addition, we have on-going work related to cyber CIP efforts in several other areas including: (1) Cybersecurity-related standards used by critical infrastructure sectors, (2) Federal efforts to recruit, retain, train, and develop cybersecurity professionals, and (3) Federal efforts to address risks to the information technology supply chain.

Federal Capacity to Protect Against Cyber Threats Needs to Improve

In addition to improving our National capability to address cybersecurity, Executive branch agencies, in particular DHS, also need to improve their capacity to protect against cyber threats by, among other things, advancing cyber analysis and warning capabilities and strengthening the effectiveness of the public-private sector partnerships in securing cyber critical infrastructure.

- *Enhancing cyber analysis and warning capabilities.* In July 2008, we reported that DHS's US–CERT had not fully addressed 15 key attributes of cyber analysis and warning capabilities.[13] As a result, we recommended that the Department address shortfalls associated with the 15 attributes in order to fully establish a National cyber analysis and warning capability as envisioned in the National strategy. DHS agreed in large part with our recommendations and has reported that it is taking steps to implement them. We are currently working

[10] GAO, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance,* GAO–10–606 (Washington, DC: July 2, 2010).

[11] GAO, *Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed,* GAO–11–117 (Washington, DC: Jan. 12, 2011).

[12] GAO, *Cybersecurity: Key Challenges Need to Be Addressed to Improve Research and Development,* GAO–10–466 (Washington, DC: June 3, 2010).

[13] GAO, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability,* GAO–08–588 (Washington, DC: Jul. 31, 2008).

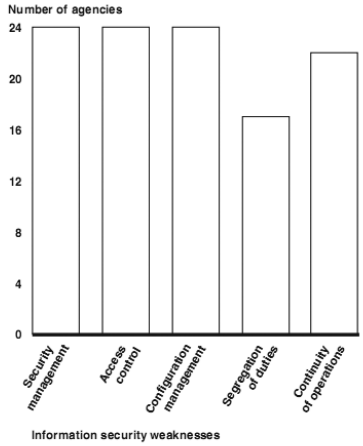
with DHS officials to determine the status of their efforts to address these recommendations.

- *Strengthening the public-private partnerships for securing cyber critical infrastructure.* In July 2010, we reported that the expectations of private sector stakeholders were not being met by their Federal partners in areas related to sharing information about cyber-based threats to critical infrastructure.[14] Federal partners, such as DHS, were taking steps that may address the key expectations of the private sector, including developing new information-sharing arrangements. We also reported that public sector stakeholders believed that improvements could be made to the partnership, including improving private sector sharing of sensitive information. We recommended that the National Cybersecurity Coordinator and DHS work with their Federal and private sector partners to enhance information-sharing efforts, including leveraging a central focal point for sharing information among the private sector, civilian government, law enforcement, the military, and the intelligence community. DHS officials stated that they have made progress in addressing these recommendations, and we will be determining the extent of that progress as part of our audit follow-up efforts.

Federal Agencies Have Not Addressed Persistent Control Weaknesses or Implemented Effective Information Security Programs

Federal systems continue to be afflicted by persistent information security control weaknesses. Specifically, agencies did not consistently implement effective controls to prevent, limit, and detect unauthorized access or manage the configuration of network devices to prevent unauthorized access and ensure system integrity. Most of the 24 major Federal agencies had information security weaknesses in five key internal control categories,[15] as illustrated in Figure 1. In addition, GAO determined that serious and widespread information security control deficiencies were a Government-wide material weakness in internal control over financial reporting as part of its audit of the fiscal year 2010 financial statements for the United States Government.

Figure 1: Information Security Weaknesses at Major Federal Agencies for FY 2010



Source: GAO analysis of agency, inspector general, and GAO reports.

[14] GAO, *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed,* GAO–10–628 (Washington, DC: July 15, 2010).

[15] The five internal controls are access controls, which ensure that only authorized individuals can read, alter, or delete data; configuration management controls, which provide assurance that only authorized software programs are implemented; segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations; and an agency-wide information security program (security management), which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented.

Over the past several years, we and inspectors general have made hundreds of recommendations to agencies for actions necessary to resolve prior significant control deficiencies and information security program shortfalls. For example, we recommended that agencies correct specific information security deficiencies related to user identification and authentication, authorization, boundary protections, cryptography, audit and monitoring, physical security, configuration management, segregation of duties, and contingency planning. We have also recommended that agencies fully implement comprehensive, agency-wide information security programs by correcting weaknesses in risk assessments, information security policies and procedures, security planning, security training, system tests and evaluations, and remedial actions. The effective implementation of these recommendations will strengthen the security posture at these agencies. Agencies have implemented or are in the process of implementing many of our recommendations.

In addition, the White House, OMB, and selected Federal agencies have undertaken Government-wide initiatives to enhance information security at Federal agencies. For example, the Comprehensive National Cybersecurity Initiative, a series of 12 projects, is aimed primarily at improving DHS's and other Federal agencies' efforts to reduce vulnerabilities, protect against intrusion attempts, and anticipate future threats against Federal Executive branch information systems. However, the projects face challenges in achieving their objectives related to securing Federal information, including better defining agency roles and responsibilities, establishing measures of effectiveness, and establishing an appropriate level of transparency. These challenges require sustained attention, which agencies have begun to provide.

In summary, the threats to information systems are evolving and growing, and systems supporting our Nation's critical infrastructure and Federal systems are not sufficiently protected to consistently thwart the threats. Administration and Executive branch agencies need to take actions to improve our Nation's cybersecurity posture, including implementing the actions recommended by the President's cybersecurity policy review and enhancing cyber analysis and warning capabilities. In addition, actions are needed to enhance security over Federal systems and information, including fully developing and effectively implementing agency-wide information security programs and implementing open recommendations. Until these actions are taken, our Nation's Federal and non-Federal cyber critical infrastructure will remain vulnerable. Mr. Chairman, this completes my statement. I would be happy to answer any questions you or other Members of the subcommittee have at this time.

Mr. LUNGREN. Thank you very much. We will now start a round of questioning, and I yield myself 5 minutes.

Mr. Reitinger, it is so easy to be a Monday morning quarterback. As we look at what is happening in Japan, you see the effects of one of the largest recorded, most powerful earthquakes in history, a tsunami that, if you watch it via the internet, if you watch it via YouTube, you see something that is stronger than any words could present. Then you see the resulting failure at the nuclear power plants. I wonder if Japan, in analyzing threats, would ever have seen that triple whammy scenario.

So I wonder what is it that you worry most about, Mr. Reitinger? The only reason I ask you that is, I think we need to do something to get a sense of urgency about this particular subject matter, not only in the Congress, but in the public at large. So what is the most serious threat that you see to our critical infrastructure as a result of something that may visit it by way of cybersecurity, or a lack of cybersecurity, an invasion of our cyber system, penetration of our cyber system.

Mr. REITINGER. Thank you very much, Mr. Chairman.

I would like to take that in a slightly different direction, if I might. The threats are very serious, but I think it is somewhat difficult to say that this particular vector of attack is greater than this particular vector. Certainly I do worry very much about things like attacks on control systems, where it is not just, well, we can't get access to our data, but we can't have the power on; or it is not just we can't get access to our data or somebody access to our data,

somebody may have filled with our data, not just attacks on confidentiality, but integrity. So if someone got access to a major medical database and changed the contents of it, that could have significant consequences in terms of human life for a large number of people.

But what concerns me the most is not any of those particular things, it is what you started out your question with. Was Japan fully prepared? As much as they prepared, were they prepared? Are we now prepared for that type of cyber attack and are we doing the things that we need to do now to be ready when and if that sort of event takes place? We have done considerable things to raise the priority of cybersecurity.

Just last year, the Ranking Member mentioned the first-ever Quadrennial Homeland Security Review which identified cybersecurity as one of the top mission areas for the entire homeland security enterprise on a par with protecting our borders and having domestic security and providing resilience to disasters. On a par with those things, cybersecurity is just as important. But are we, as a Nation, going to do the things that we need to do to make sure that we have got the capabilities and ability to respond across the public and private sectors? Are we going to keep the focus and move forward rather than waiting to respond when it is too late?

Mr. LUNGREN. Mr. Wilshusen, looking at your report and your comments, your suggestion is we are not doing all that we need to do. Can you outline, in your opinion, for instance, what is hindering DHS's cybersecurity mission right now?

Mr. WILSHUSEN. Well, I think there are probably a couple of issues. Just to echo what Mr. Reitinger mentioned, too, is that preparation is key in order to address these threats because often you may not know exactly what will happen, but you will need to be able to respond to them and hopefully take corrective action before the need occurs.

One of the things that DHS could do to help the private sector and others to better protect their systems is to provide clear, actionable, and alert threat information and share techniques with the private sector to improve their security.

Mr. LUNGREN. Is that not being done, in your opinion, to the extent necessary?

Mr. WILSHUSEN. Well, we recently completed a review in which we asked private sector organizations what its key expectations are of the private sector/public partnerships. Over 98 percent of the respondents indicated that having actionable and timely threat and alert information was essential to a great or moderate extent, but only 27 percent felt that they were actually receiving that type of information to a great or moderate extent.

So clearly, one of the actions that DHS can do is to help provide value-added services to its constituents and to the private sector. It is attempting to and has taken actions to help improve its cyber analysis and warning capabilities, but as Mr. Reitinger mentioned in his opening remarks, more needs to be done.

Mr. LUNGREN. My time is up.

The Ranking Member is recognized for 5 minutes.

Ms. CLARKE. Mr. Reitinger and Mr. Wilshusen, DHS has many detractors on any number of issues, but we want to make sure that

the right people are tasked with doing the job of addressing cybersecurity to our critical infrastructure. The other agencies in the Federal Government with considerable cybersecurity expertise are the NSA and the DOD. Is DHS the proper agency to lead Federal cybersecurity efforts? Is there another Federal agency that should do this?

Mr. REITINGER. Thank you, ma'am. I think I will start, if that is all right.

I think DHS absolutely is the right place to lead efforts with regard to Federal civilian systems and the private sector. I would like to respond in part of response to your question to what Greg had indicated. There is a long way to go in terms of being able to share the right information with the private sector. We have made significant strides. If you just take the last couple of years, at the start of fiscal year 2009, DHS and the entire National Cybersecurity Division had, I think, 38 people at the start of the year. Over the last 2 years, we have roughly tripled that, and then roughly doubled it in 2009 and 2010, so we are up to about 240 right now. In the President's request in the fiscal year 2012 budget, we grow that to a little more than 400 people.

So we are significantly expanding our people, and expanding our people expands our capabilities. I think Greg would tell you that we have done a lot.

We have had significant successes, for example, in terms of sharing actionable information. We are in the course of a pilot right now with the financial services sector where we share information—and we partnered with DOD and the financial services sector for this. We have shared literally hundreds of pieces of actionable information with the financial services sector, which has also shared hundreds of pieces of information back to us. We then take that information, it comes back to us in an itemized form, we can glean data from it and pass that out. So we are moving forward on actionable activities that actually add value.

There are lots of roles to play here. DOD has an essential role to play protecting military systems and providing a core and deep technical expertise in the National Security Agency and Cyber Command on which all of us in appropriate cases rely. We at DHS have our own expertise. For example, we have deployed, in the much messier environment of the Federal civilian infrastructure, EINSTEIN 2, which is a system designed to detect attempts to break into Federal civilian systems. Just last year, it detected over 5.4 million events. We have not done that in a unitary network that is subject to command and control, but in, so far, 15 of 19 different major Federal agencies and at four internet service providers.

So we have developed the expertise on how to act in that environment, move forward to protect security, and to protect privacy at the same time.

Mr. WILSHUSEN. I would just like to add that DHS is building out its capabilities to provide services to its constituents. It has also received responsibility for providing increased oversight and assistance to other Federal agencies in implementing their information security programs and practices.

One of the issues confronting DHS, at least as we see it, do they have the proper authorities to do that? There are challenges associated with one agency providing oversight over another agency. At present, under the Federal Information Security Management Act, many of the authorities are granted to the Office of Management and Budget. But last year, in July, OMB assigned some of those responsibilities over to DHS, and DHS is working to build out its capacity to perform those services.

Certainly, as you mentioned before with DOD and NSA, they have a high level of skill and capabilities in this area. To my knowledge, they have been working with DHS to some extent in transferring some of those skills and abilities as DHS builds out its own capabilities.

Ms. CLARKE. Just following up, Mr. Reitinger, on the EINSTEIN issue, the National Cybersecurity Division is currently planning to deploy five EINSTEIN monitors or five key nodes in the dot-gov domain that will be used to prevent and detect intrusions on computer systems. If the continuing resolution is adopted by Congress and you don't receive your requested funds for 2011, how would it affect this much-needed project and the request for $226.6 million in the fiscal year 2012 budget?

Mr. REITINGER. Thank you, ma'am.

I think the proposal under H.R. 1 would cut roughly $60 million from the entire NPPD budget. It is actually a budget cut not specifically to cyber, but more broadly to NPPD, but there is no way in our budget to do that without a cut to cyber. So a big chunk of those resources would, in fact, be drawn from the resources we would use to deploy what you are referring to, the EINSTEIN 3 system, and it would adversely affect the time line for deployment of those sensors, yes, ma'am, and our ability to provide advice and assistance to agencies on the data that we receive.

Ms. CLARKE. Thank you very much.

I yield back, Mr. Chairman.

Mr. LUNGREN. Mr. Reitinger, you are not here to testify as to whether or not we should have another month in which we have a $228 billion addition to the debt, are you? I didn't think so.

Mr. Walberg is recognized for 5 minutes.

Mr. WALBERG. Thank you, Mr. Chairman. Thanks to the panel for being here talking about an area that is expanding my mind daily, as I think about it—so far not causing me a lot of loss of sleep because I know that there are people who are thinking about it regularly, but I appreciate your testimony this morning.

The question I would just begin with to each of you is a short question with an answer that probably I would ask you to consider answering in relationship to what you know today and what you perceive today.

In which sector could a cyber attack do the most damage?

Mr. REITINGER. So, sir, I am somewhat hesitant simply because it is hard to say that one sector grown large is critical from top to bottom whereas another sector is not critical from top to bottom. There are, however, critical entities in many sectors, and some of the sectors we worry most about are, for example, financial services and electric power, primarily because those are sectors, along with information and communications, where you notice adverse effects

in milliseconds—and I mean that, milliseconds—as opposed to seconds, minutes, hours, or days.

Mr. WALBERG. Thank you.

Mr. Wilshusen.

Mr. WILSHUSEN. I would agree with Mr. Reitinger's remarks, particularly as it relates to the financial services and electrical power sectors.

There was an incident a couple years ago at a power plant, nuclear power plant in Alabama. Now this was an unintended incident, it was not due to a cyber attack, but it does represent and illustrate the impact that could occur from such an attack. It was due to an equipment failure on a network that was connected to one of the control systems. Through a series of events that occurred as a result of that equipment failure, the plant had to bring down its nuclear reactor for a time. Its due to, in part, because of the interconnectivity of these systems to control systems. So it can have a potentially devastating effect.

Certainly on the financial services side, there have been numerous reports where literally millions of dollars have been lost and absconded with through cyber attacks.

Mr. WALBERG. Thank you.

Mr. Reitinger, moving on from that—and I would suggest that your answers coincided with my thoughts, as elementary as they may be, in talking with energy providers and financial institutions in the past several weeks, that just the effect of a keystroke is amazing.

But let me ask you, Mr. Reitinger, are private sector entities responsive to the efforts the Government makes with them to warn of threats and mitigate the consequence of attacks? What is the experience there?

Mr. REITINGER. I think, sir, you would find that the experience in the private sector is similar to that in Government agencies. There are a lot of entities who get it and some who don't. The private sector has created wholly new technical capabilities over the last 10 years and has itself built new ways of working together and sharing information, not only expanding their information sharing and analysis centers, but creating other mechanisms to work together.

All that said, we are not yet where we need to be in terms of broad awareness, but within the business community and among individuals, in terms of what the threat is and what actions they need to take. One of the things that we are trying very much to do in the Department of Homeland Security is do less of the talking to ourselves, and as we raise awareness, making sure we are talking to the right people, talking not just to CISs, chief information security officers or chief risk management officers, but talking to chief financial officers and chief operating officers, the people who cut the checks and say this will affect your bottom line.

There is broad willingness and interest across the public and private sectors to work together. There is still a long way to go to have uniform action.

Mr. WALBERG. Mr. Wilshusen, you mentioned that the Government must improve the public-private partnership by improving in-

formation sharing. What are some specific recommendations you would have?

Mr. WILSHUSEN. Well, one is, as I mentioned before, for DHS, in its role as a key focal point with dealing with the private sector, is to provide actionable, timely notices of either warnings, threat warnings, as well as alerts of specific actions currently underway. That has been one of the key services that the private sector organizations have indicated that they expect to receive but have not yet fully received to the levels of expectations. So that would be one area that DHS could work on. Indeed, as Mr. Reitinger mentioned earlier, they are taking steps to address those areas.

Mr. WALBERG. I see my time is up. Thank you.

Mr. LUNGREN. The gentleman from Louisiana, Mr. Richmond, is recognized for 5 minutes.

Mr. RICHMOND. Thank you, Mr. Chairman.

I guess my question is for whoever wants to answer. Part of what at least I saw in the BP Horizon oil spill in Louisiana was that as soon as it happened, there was a clear chain of command and there was a set up protocol and people who took over at certain points. Do we have, in the event of a cyber attack, a clear chain of command with defined roles and responsibilities within Government?

Mr. REITINGER. Sir, to be frank, I think we could use further clarity. We have made significant strides in that regard. Overall, cyber incidents are going to be incredibly complex, and so it is hard to generalize. But it is clear that the President is in charge overall, that with regard to domestic response, the Secretary of Homeland Security, under her Homeland Security Act and authorities under the various Presidential directives, is responsible, and DOD is responsible for National defense. We built the mechanisms to work effectively together. We now have a National cyber incident response plan that defines roles and responsibilities, and we are going to continue to improve that as our experience develops.

We have also established a mechanism so that two of the largest players—DOD and DHS—can work effectively together, notably signing a memorandum of agreement which was driven, I will tell you, at the Secretarial level; so directly between the Secretary of Homeland Security and the Secretary of Defense to enable effective synchronization between DOD. So we have a team of senior people, are deploying a team of senior people at NSA and Cyber Command, and they are deploying two groups—one from NSA and one from Cyber Command—to our cyber operation center so they can effectively support us.

One of the things that we are doing in DHS is—and this is not just about cyber, it is also about infrastructure protection—is, as we develop capability, we are becoming an operational entity. We think it is very important that we be not about discussing, but about doing and enabling others to do. So that is where our focus is.

Mr. WILSHUSEN. I would just add that one of the key aspects to this that would also be helpful to have a straight line of chain of command is for the administration and Federal agencies to establish and update the National Policy for Securing Cyberspace. This is a document that is many years old. It has had a number of issues with it that have impeded its progress in being able to be

implemented. One thing that needs to be developed is just a clear articulation of the objectives, goals, and priorities for Federal agencies and the private sector to implement security over cyberspace and the systems that they operate.

Mr. RICHMOND. Thank you.

As I was talking to my community health centers yesterday, we started talking about electronic health records and they mentioned to me that there were 60 companies just in my area that provided those services. Then I started thinking about smart grids. Do we have an industry standard or is there a published standard that these companies have to have in relation to protecting their electronic health records? Or have we set a baseline that they have to at least adhere to to make sure that we protect people's privacy and we protect the risk of an attack in that area?

Mr. WILSHUSEN. Well, the Department of Health and Human Services, under HIPAA, issues a security rule that health care providers are required to follow certain security and privacy guidelines. So that is probably as close as anything that exists to a standard, if you will, or guidelines and requirements for protecting the confidentiality and integrity of health information.

Mr. RICHMOND. But under HIPAA, have they—I hate to put it this way, have they gotten to the level of sophistication to address cybersecurity in terms of protecting those health records? I know traditionally we just said don't leak people's medical condition, don't publish it, you have to protect it and put it in a safe place. But now when we start going to electronic health records, the question is whether somebody has put out the technical guidelines and the technical responsibilities to make sure that at least those companies are not easily hacked. That will be my question, and I yield back, Mr. Chairman.

Mr. WILSHUSEN. Well, the security rule does provide some guidelines, but probably not to the level that you are referring to in terms of the very detailed technical standards that may be required.

One of the issues that also comes up is in terms of data interoperability between various different health organizations and States to make sure that this health information is actually interoperable among different States as they develop their own individual standards. So that is another issue that is attendant to the one you are asking about.

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

Mr. Meehan is recognized for 5 minutes.

Mr. MEEHAN. Thank you, Mr. Chairman. Thank you to each of our panelists for their very revealing testimony today.

Let me ask both of you, 15 million reports in the course of a year, and yet we are trying to communicate with the private sector simultaneously, particularly those with these control systems. How do you triage to know what to communicate down the line and say this is something we ought to be reaching out to without becoming a point in time where you are—what is the old adage—crying wolf and they don't know when to really be alerted?

Mr. REITINGER. Sir, I would say you have to do a couple of things. One, you broadly have to find the broader points of influence. In a time that we all have those scarce resources, what is the

most effective way to institute protections to get the private sector not only to understand the threat, but implement the threat? So we focus very much on that.

You try to have broad campaigns. So one of the things that we did this year for the first time as a response to the President's Cyberspace Policy Review, instead of just having an annual Cybersecurity Security Awareness Month, we have now got an annual campaign, the "Stop. Think. Connect." Campaign, which we are advocating for. It was developed—not by DHS, but actually by a partnership. That is something a partnership can do; it is people in the private sector and the public sector working together to come up with a message that we can all work together to implement, something fairly actionable.

The last thing is that you do have to make choices, you do have to triage. That is something we do generally in the space. We have 5.4 million events. You can't look in detail at every one of them. You have to figure out fairly rapidly, look for indicators for what are the most severe? You try to expand our capabilities.

One of the things we have done in DHS is established fly-away teams. So we have a team of people that we can deploy if there is a significant incident in at a private sector company and they need our assistance.

In some sense it is because of the act, in some sense it is because of a prioritization, that team is typically deployed for control systems-type incidents because that is one of the things that we worry about significantly. So there are a lot of processes that one has to go through to try to figure out where you are most effectively applying resources to the effect you need.

Mr. MEEHAN. Do you agree with that sort of assessment?

Mr. WILSHUSEN. Yes, I would.

Mr. MEEHAN. The thing that really strikes me again is the interoperability. We keep talking about these control systems and the capacity to be able to impact entire areas which are interdependent. How can we create the kind of requirement, so to speak, from the private sector to collaborate with you to be able to, as we say, meet some kind of National policy standards or objectives so that we are working together? We have effectively independent agencies that have oversight over critical pieces of this infrastructure which are at risk.

Mr. REITINGER. So, sir—I feel like I keep jumping ahead of Greg. Do you want to go first or I will?

I would say there are a number of things we need to do. We at DHS are focused on executing within our existing authorities to accomplish that mission. There are a number of things we can do. We talked a lot about awareness, so raising awareness among the companies is a key part of this. As Greg has indicated, sharing classified and unclassified threat information so that they are really sensitized to what the issues are.

Second, we can work on things like helping develop standards and working with the private sector to make sure that they have available solutions so that there is a known path to better security.

Mr. MEEHAN. My time will run out, but are there minimal standards right now that we have in the industry that we can expect people to abide by so that at least there is some kind of a baseline

that we can expect collaboration that they will address within their own institution so that they are capable of communicating with you about these issues?

Mr. REITINGER. So there are many standards, sir, of differing degrees or prescriptiveness, if you will, and effectiveness. One of the things that I don't think we have right now is what one might think of as a baseline ability to say across all of the critical infrastructures we are meeting the standard that we need. So one of the things that we are doing is working with not only other agencies within the Federal Government so that they are aware of what the requirements are, but we have, in one case, DHS has specific authority, and that is for the chemical facilities sector, or the chemical sector where we have put in a risk-based performance standard into the existing CFATS regime related to cybersecurity. We will be continuing to look at that going forward to make sure that it meets National requirements.

Mr. WILSHUSEN. If I may add, we have an on-going engagement right now looking at what standards are in effect at various different critical infrastructure sectors and to assess, to the extent that those standards exist, whether they are voluntary; and how those sectors either enforce or assure that their members actually implement those standards. We expect to be reporting out on that later this year.

Mr. MEEHAN. Thank you, Mr. Chairman.

Mr. LUNGREN. I will just tell the gentleman that we will shortly schedule a markup on the CFATS bill so that we will have that issue going forward.

I understand Mr. Keating has no questions at this time, so Mr. McCaul is recognized for 5 minutes.

Mr. MCCAUL. Thank you, Mr. Chairman. Phil, it is good to see you again. Thank you for your hard work on the CSIS Commission. It is a great report, outstanding.

I mean, the threats are real, we all know what they are—the power grids, financial sectors. You know, when I was Ranking Member of this subcommittee two Congresses ago, we held hearings and talked about what is the coordination between DHS? DHS has a primary mission to defend. Are they talking to DOD or NSA that has the offensive capability, not that one is charged with defensive, are those coordinating as well?

I will say, I think, DHS has come a long way since those hearings, and that is very good news. I noticed, Phil, in your testimony you talked about an MOU that has been signed between DHS and the DOD, and I was very glad to see that. Can you explain how that is working? Also, do you anticipate doing something similar with NSA?

Mr. REITINGER. Absolutely, sir. So I talked a little bit about that before. We signed, at the Secretarial level, an MOA, a memorandum of agreement—sorry, I fall back into acronyms too much—between the Department of Defense and the Department Homeland Security. There are two points of contact on that; one is me, and the other is Dr. Jim Miller, who is the Principal Under Secretary of Defense for Policy at DOD. Under that agreement, DHS, so that we can stay fully synched with our partners in the Department of Defense, has and is deploying a team of people to Fort Meade that

will be led by a DHS senior, who is currently Rear Admiral Mike Brown, who has been in the Department of Homeland Security on detail from DOD for a number of years.

He will have a team of people that will comprise first a joint coordination element to do joint planning at DOD, make sure we can stay operationally synched, a group of people who are going to work with NSA on its technology, and another group of people who will be embedded in the NTOC at NSA so that we have full assay of the NSA's knowledge of the threat.

NSA and Cyber Command are both deploying teams of people to our Cyber Operation Center to support our domestic cyber operations. So there will be a cryptologic support group from NSA and a cyber support element—I am more comfortable with CSG and CSE, but those are what they are called—from Cyber Command that will directly support us. We are in the initial stages of developing these capabilities, but it is already working very well. I would also say that those are not the only means that we have to coordinate. So we literally hold a weekly SVTC, a secure video teleconference, with our partners in DOD to make sure we are staying coordinated. We work with them at deputies committee meetings and lots of other administrative policy and other processes. So we have come a long way between these two departments in our ability to support each other and our respective mission spaces.

Mr. MCCAUL. That is certainly good news, and I do want to commend you for that. Again, from two Congresses ago, that is great progress, and I am very glad to hear that. They have the assets, the expertise, and the capabilities, so it makes no sense for them not to work with you and share that.

Private sector sharing threat information, it is always difficult for the private sector to share that with the Federal Government. The incentives are still lacking, I think, to some extent. They have a duty to their shareholders, they don't want to report this kind of stuff. How do you incentivize them to do that? Would an exception to FOIA be helpful in terms of that threat information not being subjected to a FOIA request?

Mr. REITINGER. With regard to at least some information submitted under the Protected Critical Information Infrastructure program, the PCII program, there is a FOIA exception. The issue I think is a little broader, and that is that there remains a lack of clarity about the costs and risks of sharing information from the private sector to the Government. So sometimes one has the problem that when the private sector and Government want to talk—I think generally if something is happening, the private sector will lean forward to figure out a way to share information, as will the Government. Because when you get operators talking with operators, they have a problem to solve. If it is more on-going, the problem is, nowadays, if you get together and you want to work together, you want to share information, not just to share information to solve a particular problem, sometimes the first thing you have to do is call the lawyers into the room. You and I, sir, are both lawyers, we love lawyers, but——

Mr. MCCAUL. I wouldn't necessarily say that.

Mr. REITINGER. So we have some internal processes going now to try and generate some clarity with the private sector about what

the rules are so that you can have a more rapid and effective conversation.

Mr. MCCAUL. Last, if I could indulge the Chair, the National Policy for Cyberspace—it was mentioned earlier—sir, the last one was developed in 2003, I think one of the recommendations we had with the Commission was to develop a National policy. That is within the jurisdiction and authority of the White House. Can you demonstrate why that is so important and so critical?

Mr. REITINGER. Well, I think having a National policy is critical. I would personally favor, while I think we knew new ways to do things, focusing very heavily on implementation. We at DHS are working right now on the strategy which will underlie the cybersecurity part of the Quadrennial Homeland Security Review that the Ranking Member brought up. So for us this is mission four or cybersecurity across the Homeland Security enterprise. We are working now across Government and with the private sector to develop that strategy that will roll out to the broader National strategy.

Mr. MCCAUL. Thank you so much.

Mr. LUNGREN. I want to thank our panelists for not only your oral testimony here today but your written testimony. You have helped us considerably.

Mr. Reitinger, and also in classified briefings, I just want to tell you that members of this panel very much appreciated your participation and the participation of others, and that has helped us a great deal.

I will be calling on both of you in the future to help us a little bit more as we go forward on an issue that will not go away and only needs greater clarity and greater visibility. So we thank both of you.

Now, we would move to our second panel, and I know it will take a little while for the three of them to get there.

We are very pleased to have our second panel. We have outstanding panelists in both panels, and we very much appreciate your time and your effort and the knowledge that you are relaying to us here today.

Dr. Phyllis Schneck is the vice president and chief technical officer of Global Public Sector for McAfee. She also serves as a volunteer as chairman of the board of directors of the National Cyber-Forensics & Training Alliance, which is an important partnership between Government, law enforcement, and the private sector for information analytics and has been used to prosecute over 150 cyber criminals worldwide.

Earlier Dr. Schneck worked as vice president of Threat Intelligence at McAfee and was responsible for the design and application of McAfee's internet reputation intelligence. She has Ph.D. in computer science from Georgia Tech where she pioneered the field of information security and security-based higher-performance computing.

Thank you for being here.

Dr. James Lewis is a senior fellow and program director at CSIS where he writes on technology, National security, and the international economy.

Before joining CSIS, he worked in the Federal Government as a Foreign Service officer and as a member of the Senior Executive

Service. Most recently he was the project director of CSIS's Commission on Cyber Security for the 44th Presidency. That report has been downloaded, I understand, more than 40,000 times, so no secrets there. He received his Ph.D. from the University of Chicago in 1984.

Mischel Kwon is an IT executive with more than 29 years of experience ranging from application, design, and development to building organizational and National level computer emergency instant response and readiness teams. She is most recently the vice president of Public Sector Security for RSA, the security division of the EMC Corporation, and prior to that, she was the director of the United States Computer Emergency Readiness Team, US–CERT, at DHS.

We welcome all of our witnesses. We are pleased that you are able to share your perspective with us. As I said, your written testimony will be made part of the record. We would like to recognize each of you in order for 5 minutes, and I know that is a short period of time, but we will try and stay with that as much as possible and then ask you questions.

So, first of all, Dr. Schneck.

STATEMENTS OF PHYLLIS SCHNECK, VICE PRESIDENT AND CHIEF TECHNICAL OFFICER, MC AFEE INC.

Ms. SCHNECK. Good morning.

Chairman Lungren, Ranking Member Clarke, and other distinguished Members of the subcommittee, thank you for requesting McAfee's views on cyber threat to critical infrastructure and the American economy. It is an honor and a pleasure to be part of the process and to be here today.

Your committee is playing a vital role in helping to define the contours of cybersecurity debate, and your aim to write thoughtful and incentives-based legislation must be commended.

As you mentioned, I focused my entire career on cybersecurity, looking at both the technology and the applications and certainly the trust engaged in public-private partnership and the need for more information sharing.

McAfee is the largest dedicated cybersecurity company in the world, and we are also a wholly-owned subsidy of the Intel Corporation. We protect the cyber spectrum, from the biggest computers and the big cloud computing, as we all refer, to the smallest components, even down to our cell phones or airplane avionics systems and our cars and certainly now to the chip.

My testimony will focus on the following key areas: The evolution of the cyber threat landscape; McAfee's Global Threat Intelligence Solution; and the paradigm change that we need to make in order to protect our cyber infrastructures and thus our global critical infrastructures; two major cyber security events, advanced persistent threats that we have seen, these are just two of many, many, just two that have been vocalized; and certainly some policy recommendations to improve public-private sector information sharing.

Our adversary is strong. Our adversary is smart. They act faster than we do. They have full funding, in many cases, from governments, from nation states. They have malicious intent, and they

don't have the intellectual property barriers that we do. They don't have the legal barriers that we do to execute. They are criminals; there is nothing to lose.

So when you look at the landscape from 20 years ago and you look at "antivirus," all of the adversary's ability over the past 2 decades, all of the damage we have talked about this morning, has been enabled by malicious code, the ability of an adversary to execute their will somewhere else, and whether it causes, as in the old days, just something to prove that somebody can do something all the way to financial organized crime with a financial motivation, and now, as we are seeing, government-structured or nation-state attacks that look for destruction and/or the taking of intellectual property.

As we look at how we fight that, a signature will not beat this adversary. Signature was a legacy model. We should know about the attack. We will protect everybody, and boom, they are fine when they get it, sort of like a vaccination.

That doesn't work anymore. We need a full paradigm shift to retake the global cybersecurity picture that we have as a private industry and Government and infuse that into our network fabric, again from cloud to chip, where the enemy's will is blocked before it reaches a target.

When you think about global threat intelligence and what we mean by that, McAfee and other companies in the IT infrastructure and other infrastructures have the ability and have developed very sophisticated information-gathering capabilities where we have a weather map, a cyber weather map of events that happen all over the world, an understanding of traffic volumes, an understanding of what machines are doing, what harm and to where, where they are targeting, where malicious code that looks just like other malicious code is being sent.

We have to react in two ways: We have to react first and foremost to beat this adversary in milliseconds. The one thing this enemy can't do is understand how the entire system works and block it in real time, so the disease never reaches your body or your body can fight the disease in real time without understanding the name of the germ first.

The second thing we have to do is better enable ourselves to share information at the human level. While that is not real time, it helps us understand the motivation, understand future targets and, first and foremost, protect ourselves.

We looked at two major threats over the past couple of years and led the investigations at McAfee. There are many others like this, but first one was Operation Aurora, same name as the diesel generator explosion at INL; however, we kept the name for this one. That is the name the bad guys gave it. It is in the file path.

This was the most sophisticated event we have ever seen targeted toward the private sector. They usually save this for our friends in Government. We estimate it took teams of people many weeks to target the 20 or so companies they looked for, the information they wanted to get, and, most powerfully, the people in those companies that had an access to code stores of that size, meaning the people that tested the code, the people that have to see all of it working together.

They exfiltrated or took the copies of the code out to servers placed in different countries, and they are using that likely today. Many attacks exist that look just like this today. They lurk; they are often called advance persistent threat.

The other one we recently discovered and investigated was called Night Dragon, similar set up but less sophisticated, again one of many. But they were looking specifically at architectural plans for pipelines in the oil and gas sector, and this one was around the world.

Leading to the policy recommendations, the private sector needs some stronger protections to share information with Government and law enforcement. It was said in the earlier panel, in the middle of the crisis, the operators will talk, and they do. But we need to be better protected.

We and other companies put little pieces of the puzzle together, and we get a very big picture, and we want to share that with our colleagues in Government and in law enforcement.

We want to do that faster. We can't. It creates in many cases material information that affects shareholders, companies' bottom lines, and it can breach trust. We need much stronger protection, so that when someone in law enforcement, as they did, called me up and says, why didn't I have this yesterday when you knew it, my answer doesn't have to be, because I could get fired.

We have to beat this adversary, and we have to—we all of the—we have a lot of the information we need among the private sector to use the great collaborative organizations that DHS and the FBI and others have created for us with the private sector. Great construct exists. If we can put more information into those, we can use those constructs to their fullest potential.

So, in conclusion, I do want to thank you very much for having us today, for being a part of the process. McAfee is very committed to working with the U.S. Government to solve the cybersecurity challenges and to beat this adversary.

[The statement of Ms. Schneck follows:]

PREPARED STATEMENT OF PHYLLIS SCHNECK

MARCH 16, 2011

Chairman Lungren, Ranking Member Clarke, and other distinguished Members of the subcommittee, thank you for requesting McAfee's views on the cyber threat to critical infrastructure and the American economy. Your committee is playing a vital role in helping to define the contours of the cyber security debate, and your aim to write thoughtful, incentives-based legislation must be commended.

My name is Phyllis Schneck and I have dedicated my entire professional career to the security and infrastructure protection community. My technical background is in high performance computing and cryptography. In addition to serving as Vice President and Chief Technology Officer, Global Public Sector, for McAfee, I serve as Chairman of the Board of Directors of the National Cyber Forensics and Training Alliance, a partnership between Government, law enforcement, and the private sector for information analytics that has been used to prosecute over 150 cyber criminals world-wide. Earlier, I worked as Vice President of Threat Intelligence at McAfee and was responsible for the design and application of McAfee's™ internet reputation intelligence. I have also served as a commissioner and working group co-chair on the public-private partnership for the CSIS Commission to Advise the 44th President on Cyber Security.

Additionally, I served for 8 years as chairman of the National Board of Directors of the FBI's InfraGard™ program and as founding president of InfraGard Atlanta, growing the InfraGard program from 2,000 to over 33,000 members Nation-wide. Before joining McAfee, I was Vice President of Research Integration at Secure Com-

puting. I hold a Ph.D. in Computer Science from Georgia Tech, where I pioneered the field of information security and security-based high-performance computing.

My testimony will focus on the following key areas:

- The evolution of the cyber security threat landscape;
- McAfee's Global Threat Intelligence Solution and the role it plays in enabling us to detect and remediate a wide range of cyber security attacks on our Nation's critical infrastructures;
- Two major cyber security attacks, Night Dragon and Operation Aurora, and their implications for our homeland security; and
- Policy recommendations to improve public/private sector information sharing that is essential to give the Government the capabilities it needs to respond to the modern cybersecurity challenge.

First I would like to provide a little background on McAfee and some of our cybersecurity initiatives.

MC AFEE'S ROLE IN CYBER SECURITY

McAfee, Inc. protects businesses, consumers, and the public sector from cyber attacks, viruses, and a wide range of on-line security threats. Headquartered in Santa Clara, California, and Plano, Texas, McAfee is the world's largest dedicated security technology company and is a proven force in combating the world's toughest security challenges. McAfee is a wholly owned subsidiary of Intel Corporation.

McAfee delivers proactive and proven solutions, services, and global threat intelligence that help secure systems and networks around the world, allowing users to safely connect to the internet and browse and shop the web more securely. Fueled by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

To help organizations take full advantage of their security infrastructure, McAfee launched the Security Innovation Alliance, which allows organizations to benefit from the most innovative security technologies from thousands of developers who can now snap into our extensible management platform. Today, more than 100 technology partners—large and small businesses all committed to continuous innovation in security—have joined the alliance, with more to be announced soon.

Two years ago, McAfee announced an initiative to fight cybercrime, a wide-ranging initiative aimed at closing critical gaps in assisting victims of cybercrime and preventing new events. The initiative is anchored by a multi-point plan that includes calls for action from law enforcement, academia, service providers, Government, the security industry and society at large to deliver more effective investigations and prosecutions of cybercrime.

Key elements of the plan include:

- *Education and Awareness*.—McAfee works to ensure that officials around the world have the capacity to properly fight cybercrime, while helping users build "street smarts" so that they don't become easy victims.
- *Legal Frameworks and Law Enforcement*.—McAfee works to facilitate international collaboration and mutual assistance on cybercrime among governments, industry, and non-governmental organizations (NGOs).
- *Innovation*.—McAfee works with the technology industry to provide technology solutions that stay one step ahead of the threats.

McAfee is also supportive of the National Strategy for Trusted Identities in Cyberspace (NSTIC), working with our partners in Government and industry to enable innovation for more efficient authentication and other technologies facilitating a safer and more pleasant experience for electronic transactions.

McAfee is committed to bringing the best security products and services to the market, partnering with leading IT vendors to ensure that customers have the ability to pick and choose the best solutions to close their security gaps, and giving consumers and organizations additional resources and support to fight cyber-crime ranging from organized financial crime to attacks that user the cyber infrastructure to gain access to intellectual property or physical infrastructure. Likewise, McAfee is committed to taking part in a constructive dialogue with policy makers on cyber security initiatives, as we are pleased to do in this hearing today.

THE EVOLUTION OF THE CYBER SECURITY THREAT LANDSCAPE

For purposes of this testimony, we define malware as a set of instructions for a computer that causes the computer to behave in the will of the malware owner, such as providing unauthorized access to information or systems that control physical/kinetic infrastructure. Computers execute instructions. Malware puts the enemy's in-

struction next on the list, and then the adversary controls all actions forward, sometimes hiding its presence. Malware enters a machine from a variety of ports, typically email, web, or connection-level access that is unprotected or ill advised to admit these harmful instructions. Malware can also be referred to commonly as a "virus." As in biology, when a machine has a virus it is compromised and its functions can cause harm.

Historically, security software relied on antivirus "signatures" to recognize and block malware. Once a virus was detected, a signature was developed by the security software vendor and deployed in the form of a DAT file downloaded to the security software on customers' computers. That software would then be in a position to recognize and block the malware—an approach much like a vaccine that requires advance knowledge of the threat. However, this approach is not sufficiently fast to fight today's cyber adversary, and that is why McAfee is changing the paradigm to proactive defence in real-time: to make our networks sufficiently intelligent to prevent malicious instructions from reaching the target—instead of requiring that the target be vaccinated with a signature.

Today, malware developers combine web, host, and network vulnerabilities with spam, rootkits, spyware, worms, and other means of attack. Significantly, malware is often distributed with micro-variations (polymorphism), or the ability to change quickly, with the effect that a signature developed when the malware is first discovered is ineffective against the multiple, very slightly different forms of the same malware. This is analogous to a disease mutating so that the vaccine is no longer effective. Malware may be distributed indirectly by networks of computers that have been corrupted by a criminal (a "botnet").

Criminals, terrorists, and nation states often invest great efforts to deploy their software in hundreds of thousands or indeed millions of computers owned by innocent third parties, in order then remotely to command their botnet to launch an attack on a particular set of targets. The malicious software distributed by botnets will often actively evolve to become whatever is needed by its controller and is not limited by the boundaries of antivirus labels. This means that code that appears otherwise harmless in order to be let into the network can be told to spread rapidly. This is why we refer to this type of code as a worm. It means, for example, that malware originally configured to generate spam messages can be instructed to steal banking information. Again, cyber actions rely on the execution of instructions, and a compromised machine often follows the adversary's instructions to reach out to a server in another location for its next set of instructions, which can vary widely.

By leveraging multiple threat vectors and "one-time usage," hackers are able to extend the time period in which their malware remains undetected and are thus able to steal the money, personal data, and other valuable information of users throughout the United States and the world. In this way, what might be called classic "viruses" have been blended in recent years with other types of malware and techniques used by malicious hackers intent on stealing personal data. Hackers have discovered that direct external attacks are unnecessary and risky. It is now easier to engineer malicious software that is delivered to a system remotely through various means.

Modern malware thus can no longer be classified by its perceived purpose or propagation method, because those change in an instant. Some types of software can be engineered to gain access to and maintain control over the victim's machine. Once the malware is on the system, it seeks to communicate with its controlling entity—the criminal actor. Once communication is established over the internet, any compromised machine can be instructed both to pass over any data of value to the criminal and to act as an instrument of attack against other computers and networks.

MC AFEE GLOBAL THREAT INTELLIGENCE

McAfee and other sophisticated cyber security providers have developed multi-vector, real-time, predictive protection against these more sophisticated attacks on information systems. McAfee's solution is known as Global Threat Intelligence, or GTI. Cybersecurity solutions based on this GTI approach protect the customer's computer by calculating the potential risk of a piece of content based on experience with the IP address from which it originates, the website, or other elements associated with the content in question.

Thus cybersecurity providers offer solutions enabling the customer to stop content that is analyzed as having a risk probability score that in the customer's view is "too risky" to be loaded into the memory of the customer's computer. McAfee GTI tracks the anomalous behavior and proactively adjusts an entity's reputation—its website, IP address, domain, file, network connection, and so forth—so that McAfee

products can block the threat and protect customers. Then McAfee GTI looks out across its broad network of sensors and connects the dots between the website and associated malware, email messages, IP addresses, and other associations, adjusting the reputation of each related entity so that McAfee's security products—from endpoint to network to gateway—can protect users from cyber threats at every angle.

McAfee GTI offers the most comprehensive threat intelligence in the market. With visibility across all threat vectors—file, web, message, and network—and a view into the latest vulnerabilities across the IT industry, McAfee correlates real-world data collected from millions of sensors around the globe and delivers real-time, and often predictive, protection via its security products.

Our cyber enemies are smart and fast. They maintain their knowledge of networks and techniques by freely sharing information, enjoying a lack of legal or intellectual property barriers that often block the defenders. The adversary is well-funded, often by governments, and has no barrier to swift execution. This is why our cyber infrastructures have become their play land. The ability to see a global cyber picture and to have situational awareness is what the adversary cannot do. This is where we can win—by making the network fabric reject malicious instructions in real-time, at the speed of light, before they can hit a target. This is how we can be faster than the adversary, and this is the paradigm shift from vaccines to a cyber immune system that enhances cross-sector cyber resiliency.

Our Global Threat Intelligence service as well as a number of our other products and services helped us first detect and then remediate two important global cyber security attacks—Night Dragon and Operation Aurora. These attacks are significant because they were managed by coordinated and organized teams that succeeded in extracting billions of dollars of intellectual property from leading American companies in the information technology, defense, and energy sectors—strategic industries vital to the country's long-term economic success and National security.

OPERATION AURORA

On January 14, 2010 McAfee Labs identified a zero-day (previously publicly unknown) vulnerability in Microsoft Internet Explorer that was used as an entry point for Operation Aurora to exploit Google and at least 20 other companies. Microsoft has since issued a security bulletin and patch.

Operation Aurora was a coordinated attack that included a piece of computer code that exploits the Microsoft Internet Explorer vulnerability to gain access to computer systems. This exploit is then extended to download and activate malware within the systems. The attack, which was initiated surreptitiously when targeted users accessed a malicious web page (likely because they believed it to be reputable), ultimately connected those computer systems to a remote server. That connection was used to steal company intellectual property and, according to Google, additionally gain access to user accounts.

We also discovered that intruders used a social engineering message, known as spear-phishing, to target employees with a high level of access in these companies (either software developers, quality assurance engineers, or domain administrators). The message would come from a previous acquaintance of the targeted user and would ask them to click on a web link pointing to a web server in Taiwan. As we uncovered and then reported to Microsoft, the web link hosted an obfuscated and encoded exploit for a zero-day vulnerability in Internet Explorer.

If a user had clicked on a link with Internet Explorer version 6, their machine would be automatically compromised and malicious code would be downloaded and executed stealthily on the computer. The Trojan would establish an evasive backdoor command and control channel to the same server in Taiwan through which live attackers would jump onto the system and proceed to escalate their privileges on the local machine as well as other servers within the network. As they moved rapidly through the network, they would identify and compromise repositories of intellectual property and exfiltrated data of interest out of the company. In many cases, this data included source code—the crown jewels of these information technology companies—which then could be used by attackers to discover new vulnerabilities in software that is used by the critical infrastructure industry, Government agencies, and many other organizations across the globe.

McAfee is continuing to work with multiple organizations that were impacted by this attack, as well as with various Government agencies, to address this major supply chain attack in the U.S. commercial sector.

NIGHT DRAGON

McAfee has identified a string of attacks designed to steal sensitive data from targeted organizations. Unlike opportunistic attacks, the perpetrators appear to be highly organized, premeditative, and motivated in their pursuits.

Night Dragon attacks are similar to Operation Aurora and other advanced persistent threats, or APTs, in that they employ a combination of social engineering and well-coordinated, targeted cyber attacks using remote control software and other malware. McAfee has linked these attacks to intrusions starting in November 2009, and there is circumstantial evidence suggesting they may have begun as early as 2007. Currently, new Night Dragon victims are being identified almost weekly.

Night Dragon attacks leverage coordinated, covert, and targeted cyber attacks involving social engineering, spear-phishing, vulnerability exploits in the Windows operating system, Active Directory compromises, and remote administration tools, or RATs. The attack sequence is as follows:

- Public-facing web servers are compromised via SQL injection; malware and RATs are installed.
- The compromised web servers are used to stage attacks on internal targets.
- Spear-phishing email attacks on mobile, VPN-connected workers are used to gain additional internal access.
- Attackers use password-stealing tools to access other systems—installing RATs and malware as they go.
- Systems belonging to executives are targeted for emails and files, which are captured and extracted by the attackers.

McAfee has evidence of Night Dragon malware infections in the Americas, Europe, and Asia. McAfee has also identified tactics, techniques, and procedures (TTPs) utilized during these continuing attacks that point to individuals in China as the primary source. The Night Dragon attackers are currently targeting global oil, energy, and petrochemical companies with the apparent intent of stealing sensitive information such as operational details, exploration research, and financial data related to new oil and gas field bid negotiations. As we saw with the WikiLeaks document disclosures brought about by a malicious insider, sensitive data theft can be highly damaging beyond regulatory penalties and lost revenue. And unlike Stuxnet, the tools and techniques behind Night Dragon are not specific to critical infrastructure and can be used to launch attacks against any industry.

POLICY RECOMMENDATIONS

Officials have made tremendous progress in the creation of information-sharing constructs comprising multiple agencies and the private sector. With good information, the collaboration enabled by these constructs will help us to achieve what the enemy already has: Speed and alacrity of information sharing and acting on it for high impact.

In many cases, private sector companies can solve a cybersecurity puzzle by evaluating many disparate clues. Private companies need protected ways to share their big-picture research findings with the Government without loss of trust or creation of material events for stockholders, so that the most significant cybersecurity information is expeditiously actionable. This is the human component of what Global Threat Intelligence does at machine speed. We need both in order to defeat cyber adversaries, whose aim is to harm our way of life.

Existing public/private partnerships should ensure that senior corporate and Government officials are positioned to share vital information and best practices. Among other things, this means access to sensitive (or classified) information and a secure mechanism for sharing it.

Broad-based situational awareness is vital to securing our global cyber systems and ensuring our National security. Policies that enable companies and governments to work together, using global threat intelligence (e.g., combining cyber, energy, finance, and other data) to enhance correlation and predictive capabilities, are critical to real-time responsiveness within the network switching/routing fabric. The Lieberman-Collins-Carper bill supports such information sharing by requiring the Government to share information, including threat analysis and warning information, with owners and operators regarding risks to their networks. Legislation developed in the House of Representatives would benefit from similar language.

CONCLUSION

The cybersecurity challenge faced by our country is a serious matter that requires an evolution in the way in which both the public and private sectors collaborate. Each sector has its own set of core capabilities; only the Government can implement

the complex set of organizational and policy responses necessary to counter the growing cybersecurity threat. Leading information technology companies and their customers are uniquely positioned to act as early warning systems that can identify and help address cybersecurity attacks as a real-time cyber immune system.

With the right industry-Government collaboration, networks of the future can comprise intelligence and create resiliency by instantly rejecting harmful code in milliseconds as opposed to the hours it traditionally takes to make a signature, just as our bodies reject viruses even though we may not know the name of the particular disease. Information technology companies focused on cybersecurity in particular have the resources and the economic incentives to continue to invent and develop the technologies and solutions needed to stay ahead of sophisticated cyber attackers. In the best American tradition of collaboration, the public and private sectors have made important strides to address the cybersecurity challenge and to enhance trusted working relationships. As we work together to further evolve our collaboration models, we can succeed in protecting our homeland from the threat of cyber attacks.

Thank you for asking me to take part in this hearing on behalf of McAfee. I would be happy to answer your questions.

Mr. LUNGREN. Thank you very much.

Mr. Lewis.

STATEMENT OF JAMES A. LEWIS, DIRECTOR AND SENIOR FELLOW, TECHNOLOGY AND PUBLIC POLICY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Mr. LEWIS. Thank you very much, Mr. Chairman, and thanks to Ranking Member Clarke and, of course, hello to Congressman McCaul, who was invaluable as the cochair in leading the CSIS commission. So one of the reasons it has been downloaded so many times is due to him.

This will be a good year for cyber security because of the work of this committee and others. With luck, I think in this Congress, we will see real progress in making our Nation more secure.

But this outcome is not guaranteed. We have been trying for years to secure our networks, and we have not succeeded, right.

So you have heard the litany of problems, major corporations, banks, Government agencies; they have all been victims. We have lost sensitive military information, oil exploration data, valuable commercial technologies and millions of dollars from banks.

The interesting thing about these crimes is that they are risk-free. No one has ever been punished for them, and so, of course, when you have a crime and no one gets punished, they are just going to do it again, right.

What we are doing now to secure cyberspace is not working. There has been real progress at some agencies, like DHS, but we need to rethink our approach. To put this in perspective, think about the threats we face. First, a few advanced militaries have the ability to use cyber attacks to disrupt critical infrastructure and service. They have done the reconnaissance on critical infrastructure. They have planned how to do this.

They will not launch a cyber attack because they are not going to start a war for no reason with the United States; they are deterred by our military. But if they ever did attack us, we are prepared to defend ourselves.

Terrorists do not yet have the capability to launch cyber attacks, but groups like al-Qaeda in the Arabian Peninsula are seeking to acquire these capabilities. Perhaps more worrisome, Iran and North Korea are developing cyber attack capabilities. When these

terrorist and rogue states can launch a cyber attack, they, too, will find that we are unprepared.

Cyber espionage and cyber crime are daily occurrences in the United States, and they do long-term damage to our economy and to our global competitiveness. They also help set the stage for cyber attack. Some of our opponents use cyber criminals as mercenaries, as proxy forces. Our most advanced opponents in cyber crime and cyber espionage can overpower even the most technologically sophisticated U.S. company, and we have seen many examples of that.

Agencies have made strenuous efforts, but we are not yet prepared to defend ourselves. There are three key issues that I call to the committee's attention, how to give Government a leading role in cybersecurity, how to ensure cybersecurity at critical infrastructure, something we cannot do now, and how to create international rules to reduce the risk of cyber crime and the risk of cyber war?

These are all hard problems, but they are not impossible. CSIS' Cyber-Security Commission, which Congressman McCaul helped lead, has released two reports with recommendations. Our fundamental point, and this gets to the question about the 2003 National strategy, our fundamental point is that the old approach doesn't work, and we need a new strategy that uses all the tools of American power, military, law enforcement, Homeland Security, partnership with the private sector. If we can come up with this new combined strategy, we will be able to do something effective to protect ourselves, but we are not there yet by any stretch of the imagination.

With this, I thank the committee and look forward to your questions.

[The statement of Mr. Lewis follows:]

PREPARED STATEMENT OF JAMES A. LEWIS

MARCH 16, 2010

Chairman Lungren, Ranking Member Clarke, and Members of the committee. Let me begin by thanking you for this opportunity to testify on this important subject.

Cybersecurity first came to the attention of the public in the mid-1990s, some 15 years ago. The first major policy for cybersecurity, Presidential Decision Directive 63, appeared in 1998.

In the intervening years, there has been much discussion and a few new ideas. We can get a sense of the state of cybersecurity and whether there has been any progress the United States by reviewing major cybersecurity events that have occurred since the start of 2010.

- *January 2010.*—Google announced that an attack had penetrated its networks, along with the networks of more than 80 other U.S. high-tech companies. The goal of the penetrations, which Google ascribed to China, were to collect technology, gain access to activist Gmail accounts and to Google's password management system.
- *January 2010.*—Intel Corporation also disclosed that it has experienced a harmful cyber attack at the same time.
- *January 2010.*—Global financial services firm Morgan Stanley experienced a "very sensitive" break-in to its network by the same hackers who attacked Google, according to leaked e-mails.
- *March 2010.*—NATO and the European Union warned that the number of successful cyber attacks against their networks have increased significantly over the past 12 months.
- *March 2010.*—Australian authorities say there were more than 200 attempts to hack into the networks of the legal defense team for executives from Australian energy company Rio Tinto, to gain inside information on the trial defense strategy.

- *April 2010*.—Hackers break into classified systems at the Indian Defence Ministry and Indian embassies around the world, gaining access to Indian defense and armament planning.
- *May 2010*.—A leaked memo from the Canadian Security and Intelligence Service (CSIS) says, "Compromises of computer and combinations networks of the Government of Canada, Canadian universities, private companies and individual customer networks have increased substantially . . . In addition to being virtually unattributable, these remotely operated attacks offer a productive, secure, and low-risk means to conduct espionage."
- *October 2010*.—Stuxnet, a complex piece of malware designed to interfere with Siemens Industrial Control Systems discovered in Iran, Indonesia, and elsewhere, results in significant physical damage to the Iranian nuclear program.
- *October 2010*.—The Wall Street Journal reports that hackers using "Zeus" malware, available in cybercrime black markets for about $1,200, were able to steal over $12 million from five banks in the United States and United Kingdom.
- *December 2010*.—British Foreign Minister William Hague reported (in February 2011) attacks by a foreign power on the U.K. Foreign Ministry, a defence contractor and "other British interests." The attack succeeded by pretending to come from the White House.
- *January 2011*.—The Canadian government reports a major cyber intrusion involving the Defence Research and Development Canada, a research agency for the Department of National Defence, the Department of Finance, and the Treasury Board, Canada's main economic agencies. The intrusions forced the Finance Department and the Treasury Board, to disconnect from the internet.
- *March 2011*.—Hackers penetrate French government computer networks in search of sensitive information on upcoming G–20 meetings.
- *March 2011*.—The Republic of Korea said that foreign hackers penetrated its defense networks in an attempt to steal information on the U.S.-made Global Hawk unmanned aircraft, provided to Korea as it considers whether to buy the UAV.

Major corporations, financial firms, Government agencies, and allies have all been victims, and these are just the events we know about. There are of course many more incidents stretching back into the 1990s, that include the loss of tens of thousands of pages of sensitive military information, market and exploration data worth millions from oil companies, the loss of valuable commercial technologies, and hundreds of millions of dollars from banks and other financial institutions. Classified military networks have been penetrated by foreign intelligence agencies. Best of all, from the perpetrators' perspective, no one has ever been punished for any of these actions.

This is not a record of success. Whatever we are doing is not working. Since 1998, we have repeatedly tried a combination of information sharing, market-based approaches, public/private partnership and self-regulation in a vain effort to strengthen our cyber defenses. However, despite this dispiriting record of opponent success, I feel confident in predicting that this year, the old, failed formulas will be trotted out again this year. Many of the reports and essays we see emerging now will advocate tired ideas in order to block change rather than increase cybersecurity. While individual Government agencies have made strenuous efforts to improve our cyber defenses, as a Nation, despite all the talk, we are still not serious about cybersecurity.

This is due to a reluctance to make the changes cybersecurity requires. People still advocate strategies and policies that appeared more than a decade ago and which have not worked. We have consistently underestimated the risks and damage from weak cybersecurity. Everyone is for better security, but there has always been some other objective that seemed more important.

Cybersecurity is another of those situations in American history, ranging from Pearl Harbor to 9/11, where we knew there was risk and that we were unprepared, but assumed it would never happen because America is too powerful or too big to attack.

Nothing has yet punctured this misplaced sense of invulnerability. America is still powerful, and it is easy to say that the sky is not falling and there is no need for haste. The effect of this over confidence is to make tolerable the slow erosion of our National power due to feeble cybersecurity. Some call it the "death of a thousand cuts," where each tiny cut goes unnoticed by the victim. There are warning signs that even a Nation as rich and as powerful as the United States is at risk. The challenges to our financial system and the loss of manufacturing and innovative capabilities are subjects for another hearing, but weak cybersecurity exacerbates these

problems. Business as usual means long-term decline as our economic and technological leadership is damaged by cyber espionage.

There are also two sets of risk. One is immediate and real. Two of our potential military opponents have the capability to launch damaging cyber attacks against America's critical infrastructure. The Aurora test at the Idaho National Labs and the Stuxnet worm showed that cyber attacks can do physical damage. These opponents have carried out network reconnaissance against critical infrastructure to allow them to plan their attacks. The issue for this committee is that after 12 years of information sharing, public private partnership, and voluntary action, critical infrastructure in the United States is not ready for an attack.

While these militaries have the capability to launch a damaging cyber attack, they are unlikely to do so short of an armed conflict. They are deterred by the threat of an American military response. Only if we were to get into a shooting war with them, over Taiwan or Estonia, could we expect to see cyber attacks. However, while we can deter military attack, our military strength does not deter espionage and crime in cyberspace. Deterrence not a solution for cybersecurity's most pressing problems.

Cyber terrorism is still a distant threat, but it is a threat that is increasing. Terrorists lack the capability to launch cyber attacks. If they had this capability, they would have already used it. Our original emphasis on "cyber terrorism" was wrong. The day a terrorist group gets cyber attack capabilities, they will use them. At that moment, if we have not improved our cyber defenses, they will succeed in causing disruption and damage. It is concerning to note that a few terrorist groups have expressed interest in acquiring cyber attack capabilities—the most recent was al-Qaeda in the Arabian Peninsula (AQAP). This group is worrisome. They are inventive in using the internet for propaganda and organization, and they have said one of their goals is to disrupt the American economy—this was the alleged motive for their effort using printer cartridges in air shipments. We have some number of years—I hope—before AQAP or another group, or an irresponsible nation like North Korea or Iran, acquires cyber attack capabilities, because we will not be able to deter them from attacking and our defenses are inadequate.

If there is one conclusion that we can draw from the long list of cyber incidents, it is that we are not prepared to defend ourselves. So we are vulnerable, but the risk of attack is low for the moment. As long as our opponents do not attack us, we are safe. This is not an ideal strategy for a superpower. Our current approach to cybersecurity leaves initiative and control to our opponents. It also is ineffective in stopping the slow but steady damage to our economy and to our National security that comes from cyber espionage.

Remedying the situation will take a concerted effort, but we are far from consensus on how to proceed. We will hear that public-private partnership is essential, because the private sector owns 85% of critical infrastructure. The private sector owns 100% of the airlines in the United States as well, but no one uses this as an excuse to say we do not need an air force. We will hear that the internet must be protected because it is a source of innovation. Now, in other fora, it is common to hear that the United States is lagging behind in innovation, so it is fair to ask just how much the internet has helped. Innovation is a complex process and focusing on the internet as its source is probably wrong, perhaps a last left-over form the dot-com bubble. But the notion that ability to better protect intellectual property and proprietary business information will somehow hurt innovation is bound to reappear. We will hear that technology moves too fast for regulation, but this is true only if you try to write prescriptive regulations. It is an avoidable mistake. And there will be a call for incentives, as if paying for an inadequate defense will somehow make it better.

No sector has a greater incentive than banks to protect their networks. They are a constant target. Some banks, particularly the top tier banks, have sophisticated defenses. Despite this, they are hacked. This is not surprising considering the thousand of probes they face each year, but even with all the incentives in the world and with a strong focus on cybersecurity that is matched in few other critical sectors, they cannot be secure. If the banks cannot protect themselves, why do we think other sectors will be able to do so?

The business implications for spending on cybersecurity by private companies, especially critical infrastructure companies, are straightforward. Investing in increased cybersecurity requires them to spend on nonproductive assets. They will not get an increased return on investment from this spending. There is a notion that if we could only demonstrate the scope of the losses, companies would be incentivized to recalculate the business case for cybersecurity and spend more. This may not make sense for critical infrastructure. The bulk of the losses come from the theft of intellectual property from commercial research and manufacturing compa-

nies. Critical infrastructure companies are likely experience less loss of this kind of data. The risk they face is the potential for service disruption, but before the disruption occurs, the cost may be so low as to be unnoticeable.

Additionally, it is likely that some industry sectors are more important than others for cybersecurity. Opponents may consider the defense, high-tech, or energy sectors as higher-value targets for economic espionage. Electrical and telephone grids may be high-value targets for critical infrastructure attacks, as disrupting them could have cascading effects through the economy. The financial sector may be particularly attractive as it is both a critical infrastructure—stop the flow of money and you trigger immense disruption—and attractive as a target for crime. There are indications that the financial sector and the electrical grid face increasing risk because of heightened opponent interest (whether State or criminal) in these sectors as targets.

This has implications for a National resiliency strategy. Without external incentives, companies will be unwilling to invest in redundant infrastructure to provide resilience. On the other hand, providing incentives without also being able to enforce compliance means at best, we will get a very uneven level of implementation and continued vulnerability. Incentives only make sense if increased authority for the Department of Homeland Security (DHS) accompanies them. Incentives by themselves are a give-away without benefit to security.

Incentives will not solve the problem of our reliance on a disaggregated, point cyber defense, where each network or user is responsible for their own defense. This is the worst possible defense against a skilled opponent. Every company is on its own, and they can be picked off one by one. Providing incentives without being able to coordinate our cyber defenses and ensure a common level of performance is not an improvement.

Voluntary action is also not enough. Is there a more sophisticated technology company than Google? Google has unparalleled skills and resources. The same is true for Intel, Adobe, Microsoft, and the many other companies that have allegedly been hacked. Voluntary action by even the most sophisticated tech companies is inadequate. The reason for this is simple. Pros always beat amateurs. We are asking corporations to take on the most powerful military and intelligence agencies in the world, agencies that do not observe our laws and that do not like us. It is no contest. It is like sending the company softball team against the Giants or the Yankees. Voluntary action by itself will always be inadequate against dangerous foreign opponents.

Efforts to secure the Smart Grid are a good example of the problems with a voluntary approach. Security standards published by the National Institute for Standards and Technology in August 2010 were developed by a consensus process that included 475 participants from the private sector participants. A consensus process involving 475 people is itself problematic. This is why the founders wisely opted for majority rule in the Constitution. A report by the General Accountability Office from January 2011 found that since these consensus standards are voluntary, there is no way to enforce them or even know if companies are following them. Perhaps unsurprisingly, the GAO also found that critical smart grid elements "do not have adequate security built in, thus increasing their vulnerability to attack."[1]

Voluntary action has not worked, but some argue it deserves another chance and that we should pay companies to put better cybersecurity in place, using incentives, but that we should also not tell them what to do. This is a recipe for disaster. There is no other area of National security were we rely on voluntary action reinforced by incentives. A policy of voluntary efforts for better cybersecurity reinforced by incentives is not a serious effort to protect National security against real damage and a growing threat. These proposals are best seen as intended to block reform rather than to promote cybersecurity.

Information sharing is a more difficult problem. No single agency or company knows the full range of threats we face in cyberspace. The National Security Agency, Cyber Command, and DHS have part of the puzzle, the big telecom companies have another part, the antivirus companies and big internet service providers another. If we could put these parts together, our ability to protect the Nation would be significantly improved. Perhaps 20 or 30 companies and two or three agencies would need to share information and be partners in a National defense. This would be a public-private partnership that could make a difference.

And of course, it is impossible do to this in the United States. Our laws and our policies block the one area where we could have meaningful public private partnership and information sharing that could make a difference. Some of the very organizations that stoutly proclaim the need for public-private partnership also object to

[1] GAO, Electricity Grid Modernization *(http://www.gao.gov/new.items/d11117.pdf)*.

meaningful information sharing, the one area where public-private partnership makes sense.

After 12 years of experience, we can now say with confidence that a voluntary approach to cybersecurity based on public-private partnership and information sharing is inadequate to defend America. These are elements of a comprehensive defense, but by themselves they are not enough. They must be reinforced by an active defense that uses our military and intelligence assets, by flexible regulation of critical infrastructures and internet service providers, by a strong diplomatic effort to extend the rule of law into cyberspace, and by expanding law enforcement cooperation in every country to which we are connected.

In December 2008, CSIS issued a report by its Commission on Cybersecurity for the 44th Presidency that laid out a number of recommendations for a comprehensive National approach to cybersecurity.[2] While the report was well received, the implementation of the recommendation has been slow. In February 2011, the Commission issued a second, final report[3] that assessed where progress still needs to be made. We identified ten key areas and listed the tangible steps that need to be taken. The most important of these were the need for coherent Federal leadership, clear authority to mandate better cybersecurity in critical infrastructure, and a foreign policy that used both military and diplomatic tools to bring the rule of law to cyberspace.

These are crucial areas for improvement, but each raises significant issues for the upcoming legislative debate. One issue is whether DHS or at the White House should lead cybersecurity efforts. In this case, there is not simple answer. DHS is best placed, working with the Department of Defense and the National Institute of Standards and Technology (NIST), to develop standards and regulations. DHS is best placed to work with first-party regulators—FERC, FCC, FFIEC, and others—to ensure compliance. On the other hand, the White House is best placed to develop a National strategy, to coordinate military, intelligence, law enforcement, and diplomatic activities, and to provide Executive branch oversight and guidance for cybersecurity activities and for privacy protection.

The first CSIS report discussed a new, flexible approach to regulation that gave the private sector a greater role in designing the rules while leaving enforcement to the Federal Government. Now, it is quite true that regulation done badly can be very damaging. There are countless example of that kind of prescriptive overregulation and finding ways to streamline regulation is an essential task for America. It is also true that no regulation leads to disaster. Even the strongest proponents of deregulation do not call for the elimination of the Federal Aviation Authority. All the airlines mean well and do their best, but we do not feel comfortable leaving air safety to voluntary action because lives are at stake. We do not feel comfortable saying to companies, you make the decision on whether to sell nuclear or missile technology to a foreign customer. We regulate them. Public safety and National security require it. Regulation is unpleasant, but in some cases, the alternative is worse. Cybersecurity is one such case. The approach proposed in draft legislation, which is based on the Chemical Facilities Anti-Terrorism Standards found in the Homeland Security Act, offers a reasonable approach to better cybersecurity.

Precedents for a new approach can be found in recent changes to the implementation of the Federal Information Systems Management Act Reporting Guidelines or in the Consensus Audit Guidelines developed by a consortium of Federal agencies including NSA and private organizations. These guidelines identify technical security controls that are effective in blocking high-priority attacks. They show that is possible to identify practices that improve cybersecurity and measure their effectiveness, since technology does not change too fast. I recently spoke to the Deputy Chief Information Officer of an agency that had implemented the guidelines—this was an agency that suffered major losses to hacking a few years ago—and he said the improvement in their defenses has been dramatic. I asked if the Guidelines are not getting out of date, as they are 2 years old, and he replied that not only are they are still effective, that implementing the first four guidelines stops most of the attacks. It is now possible to identify effective practices and continuously measure how well they work—if they are implemented.

A comprehensive strategy that coordinates military, intelligence, law enforcement, and diplomatic activities is essential for securing a global network. Reducing cyber crime will require a strategic, National-level approach that uses law enforcement, intelligence, and diplomacy. The most sophisticated cyber criminals live overseas, in countries that do not cooperate with U.S. law enforcement. The problem is complicated by the fact that a few countries tolerate and even encourage cyber criminals. They use them as proxies, as irregular forces to carry out operations for the

---

[2] *http://csis.org/files/media/csis/pubs/081208__securingcyberspace__44.pdf.*

[3] *http://csis.org/files/publication/110128__Lewis__CybersecurityTwoYearsLater__Web.pdf.*

Government. The provide resources and sometimes training. It will not be an easy task to get these countries to stop cybercrime, and there is little that the private sector can do.

Limitations on the use of our military and intelligence capabilities continue to weaken cybersecurity in the United States. A case from last year shows the situation. We are told that a leading American bank had its networks penetrated by Russian hackers. The hackers extracted millions of dollars. The bank, of course, said nothing publicly. But while the crime was in progress, it was detected by an American intelligence agency. As an intelligence agency with no domestic authority, there was nothing it could do other than relay the information to law enforcement agencies, a cumbersome process under today's laws. By the time this was done, the crime was over. Active defense would have let the intelligence agency detect the incoming attack on the internet backbone, on the borders of America's National networks, and stop it. Active defense could be structured to operate like NORAD, where the Air Force protects our skies, by focusing on foreign threats. It is not perfect, but it works and other nations are deploying this kind of defense against foreign attacks.

Active defense is the future of cybersecurity. It raises two key issues, the first being the need for additional privacy safeguards and oversight and the second being the division of responsibility between DHS and DOD. Stronger cybersecurity probably requires a new approach to privacy and a strengthening of existing oversight mechanisms. To give two examples, the Privacy and Civil Liberties Oversight Board, PCLOB, does not have cybersecurity in its legislative charter, nor is there Executive branch guidance (along the lines of Executive Order 12333, which governs intelligence activities) for agencies in how to perform their cybersecurity missions. Both of these reflect the need to adjust our laws and regulations to the new cyber environment.

DHS and DOD both have important and potentially complementary roles to play in cybersecurity. DHS is best placed to work with critical infrastructure and to ensure domestic preparedness. Only DOD has the capability to respond to foreign opponents. There are still coordination issues that need to be worked through, and some of these issues will be resolved only when the White House has a stronger role in cybersecurity, but the recently signed Memorandum of Understanding signed between Secretaries Napolitano and Gates is an important first step in building a coordinated defense.

The problem of international engagement is challenging, in part because for years the United States believed that cyberspace would be some kind of self-governing utopia. As the security situation worsened, as cyberspace became a new domain for conflict, and as the political implications of the new technologies became apparent, other nations have decided to extend government control into cyberspace. This trend is irreversible. The United States must engage with these nations in order to influence, if not lead, this restructuring of cyberspace governance, in order to ensure that the political values we cherish—openness, global connectivity, and freedom of speech—continue to guide development of the global network. Thinking on how to do this is at a very early stage. New kinds of expertise are required and there are only a handful of people with relevant experience. The State Department has just created a new cyber coordinator position and with the right support form Congress, this could allow the United States to regain international influence.

These are complicated issues and the account above is necessarily summary. They receive more detailed treatment in the CSIS reports. However, in drafting the final report, we found that as the prospect for change increases, so will resistance to it. People are wedded to old ideas, even if they do not work. New kinds of expertise are required for understanding cybersecurity. Above all, many still place some other priority above securing our Nation's networks.

It is this last point that worries me the most. When we look at nations that have fallen on hard times, losing their power and their international standing, very often it was because of internal problems. Often, the leaders of these countries knew what the problems were. They even knew what the solutions were, but their beliefs and reliance on old approaches kept them from making the needed changes. So far, this has been the case with cybersecurity in America. We are in a new world and face new problems that old ideas will not solve, but it is hard to give them up. Better cybersecurity is possible, but not if we continue to use failed approaches.

This puts a great responsibility on Congress and the White House. We have a real opportunity in the next 2 years to improve our cyber defense. Doing this will require leaving old ideas behind, even though many will still advocate them, and moving to a new, comprehensive approach to cybersecurity that treats it as a major component of National defense and homeland security. I thank the committee for the opportunity to testify and will be happy to take any questions.

Mr. LUNGREN. Ms. Kwon.

STATEMENT OF MISCHEL KWON, PRESIDENT, MISCHEL KWON ASSOCIATES

Ms. KWON. Thank you.

Good morning, Chairman Lungren, Ranking Member Clarke, and other distinguished Members of the subcommittee.

My name is Mischel Kwon, and I am the president of Mischel Kwon and Associates, LLC, a consulting firm specializing in technical defense security, security operations, and information assurance.

It is interesting to look at the changes and advances and struggles of IT over the 30 years of my experience. If we look out into the future, if I were to be testifying before this committee in 10 years, I predict a very different situation. No longer will governments or car manufacturers or hospitals or electric power companies be in the business of IT.

None of these organizations will have large data centers and infrastructures, e-mail servers, or application programmers. Instead, we will have IT providers, just as we have power providers and health care providers.

The cloud today is the first move to this new paradigm. This movement is our opportunity to fix many of the problems that rapid individualized IT growth has caused. We have the opportunity to build security in, to fix the IT refresh problem, to enable innovative technology, and to collapse the IT community, allowing better collaboration, communication, and sharing.

In looking to the future, it is important to recognize where we have been successful and where we are stuck. We must look at where IT is going in the next 10 years and prioritize what we are working on so that we are addressing the issues head on.

We have had significant progress over the 10 years in heightening the importance of securing our IT systems and infrastructures. We now understand the importance of policy, process, technology, and detection.

We clearly understand the need for information sharing. We now also realize we are all in the same infrastructure, the internet, and that the idea of sharing infrastructure is the wave of future.

Much-needed progress is being made in the modernization of FISMA, understanding the need for continuous monitoring and cyber scope that will enable the departments and agencies to have a real understanding of the health and well-being of the systems and networks supporting the Federal missions.

It is critical that as we move into this era of the cloud that we are careful not to create home-grown solutions but rely on the private sector and the COTS, commercial off-the-shelf products, that can accomplish the requirements needed.

Difficulties have challenged us in security governance, authorities, and information sharing. Many of these issues have been complicated because we are trying to solve the policy issues and the operational issues at the same time.

I do believe good efforts by good people with good intentions have been made at the Department of Homeland Security and across the U.S. Federal Government.

Today, many of the impediments in Federal Government that slow down efforts to improve cybersecurity are caused by a lack of clear governance structure, clear defined mission spaces, and the authorities and budgets to successfully accomplish those missions and understanding where collaboration is needed.

I do believe DHS has a primary role in cyber. Though I have not always thought DHS could handle the important and broad mission of cyber because of the maturation level of this young agency, I do believe the operational mission of US–CERT belongs to DHS, but as an autonomous, operational component, similar to FEMA, with direct reporting capabilities to the Secretary.

I believe the mission of US–CERT must be more clearly defined to enable it to be successful. It must be enabled to succeed in the important operational mission and firewalled away from the struggles of policy and relationship development. The appropriate authorities must be given to US–CERT to allow it to carry out the assigned mission.

Effective and actionable information sharing and a public-private partnership is essential for cyber today and for the future. We have made significant progress over the years but now seem to be in a holding pattern, struggling with procurement and legal issues that have frozen progress.

As we move to the new model of IT and the cloud, we will need to take two steps: One to understand how we can technologically share information more efficiently; and two, how the private sector can take a leadership role, possibly through a non-profit organization, to help free us from the holding pattern from both sides.

We are moving rapidly to the new world in IT, a new world in cyber with many opportunities. We must be prepared with a strong, well-defined operational US–CERT that has the autonomy, authority, budget to be successful in protecting the Federal-civilian space. We must defend the shared space together with the ability to share information through a healthy, public-private partnership.

Thank you very much for the opportunity to testify.

[The statement of Ms. Kwon follows:]

PREPARED STATEMENT OF MISCHEL KWON

MARCH 16, 2011

Good morning Chairman Lungren, Ranking Member Clarke, and other distinguished Members of the subcommittee. Thank you for the opportunity to testify before the Subcommittee for Cybersecurity, Infrastructure Protection, and Security Technologies.

My name is Mischel Kwon and I am the President of Mischel Kwon and Associates, LLC, a consulting firm specializing in Technical Defensive Security, Security Operations and Information Assurance.

Previously I served as the Director of the United States Computer Emergency Readiness Team (US–CERT) at the Department of Homeland Security (DHS), and as the Deputy Chief Information Security Officer and Director of the Justice Security Operations Center at the Department of Justice. Most recently I was the Vice President of Public Sector Security Solutions for RSA, the Security Division of EMC Corporation. I received my Bachelor of Science and Master of Science from Marymount University and a Master Certificate in Information Assurance from George Washington University. I was a Cyber Corps Scholar. In the nearly 30 years of my career to date as an IT professional I have been a programmer, systems developer, network engineer, program manager, and security professional.

Over the past 10 years the U.S. Federal Government has been struggling, learning, and discovering what to do about "cyber". We have been moving on a continuum

that started with the discovery of adversaries in our networks, has found us struggling with how to manage our systems through the Federal Information Security and Management Act (FISMA) and compliance, how to identify threats, attacks, vulnerabilities, and how to work together to defend our networks. As we move forward in a constantly evolving world of technology, life as we know it is changing rapidly. Soon, most companies, even Government departments and agencies, will no longer have data centers or continue to own or manage their own e-mail servers, applications, or desktops.

The use of virtualized IT infrastructure is the future. Virtualization, as the foundation of cloud computing infrastructure will enable the "Cloud" to be the provider of most IT services. You may say this is jumping ahead, but we must look at the answers to the questions you are asking with the near-term future in mind, and the near-term future is now—as many departments and agencies are already moving applications such as e-mail to the cloud, many are building private clouds, and many private sector companies are rapidly moving to the cloud. This is not only an innovative solution to a much-needed technology refresh in the civil government space, but if done correctly, could be the answer to information sharing, infrastructure-based defensive security, the cyber talent pool shortage and guaranteed lifecycle management of our infrastructure resources. No longer will companies or departments and agencies with missions different than Information Technology need to be in the "IT" business. No longer will we need to educate the heads of these organizations and have them making IT risk decisions outside of the scope of their knowledge base. We will deliver the requirements to the vendors; the vendors will then supply the appropriate infrastructure and services, with security built right into the technologies and the offerings.

This brings us to a critical crossroads in the continuum of cybersecurity. Not only are we at the point where we realize the need for governance, leadership, and cooperation between the Government and private sector in order to have a chance at combating the adversaries in an efficient manner, but we also are now at the part of the continuum where the responsibility of protecting our assets processed on IT systems—whether it is data or an operational function—will be the responsibility of the private sector infrastructure providers. This point was driven home during the initial phases of the Comprehensive National Cybersecurity Initiative (CNCI) when the Federal Government realized just how much of the internet is private sector-owned and -operated, and that even if we do better at securing Federal systems, we can't improve our Nation's cybersecurity posture without improvements in the private sector in partnership with industry. As we continue to move infrastructure and services to the "cloud", effective and lasting partnerships with the private sector must be fully embraced and leveraged.

Understanding the Information Technology roadmap that we are all moving rapidly on also increases the importance of enhancing the governance, authorities, and relationships that the Federal Government has between and among the civilian departments and agencies, the homeland security and law enforcement communities, the defense and intelligence community and of course, the private sector.

As I move into the portion of my testimony where I will be identifying obstacles and problems I have encountered during my Federal Government service, there are a few caveats and points I would like to make clear. First of all, cyber is a new field. At most, we can say this is a 25–30-year-old industry. We must understand this is going to take some time to mature. We will and have encountered issues, we will learn of new problems . . . but we must work together to overcome these challenges, quickly and effectively. Second, the Department of Homeland Security (DHS) is a new Department and because of that it struggles with the fundamental daily functions of being a Department from procurement and budgets to hiring and operations. DHS is going to take some time to develop the processes, policies, and procedures needed to run smoothly and efficiently. It will not happen overnight and will not occur without specific actions and programs to improve the baseline operations. In addition, DHS has a very broad set of missions and duties. Cybersecurity often takes a back seat to physical threats and natural disasters in the daily and weekly grind of the Department. Congress should do more to enable the cybersecurity components in the Department to operate more effectively and independently without getting bogged down in other DHS mission spaces, allowing cyber to effectively operate as an independent component; allowing cyber to separate itself from the quagmire of internal politics and jostling for resources and mindshare. Third, there are a lot of really good people who have worked this problem in the past and are working on cybersecurity challenges today. As we point out the weaknesses and problems, we must be cautious of tying the hands of dedicated security professionals who are currently doing battle on a daily basis (unfortunately not just with adversaries in cyberspace, but with the bureaucracy within DHS). We cannot afford to

forget these people. We need these qualified individuals in this young and growing field. They make sacrifices with their families, careers, and personal sanity to serve our country in trying to fix these problems. We should take the time to remember their service and take care not to diminish their contributions as we examine and address cybersecurity challenges in both the public and private sector.

During my tenure at US–CERT, we were at the very early stages of developing critical relationships with Federal civilian departments and agencies as well as relationships with the homeland security, law enforcement, defense and intelligence communities, and the private sector. It was clear there was a lack of governance and lack of authorities to carry out the poorly-defined mission US–CERT set out to accomplish. To examine this problem it is critical to break down the US–CERT mission into: (1) Protecting the Federal civilian departments and agencies, and (2) coordinating and collaborating with the private sector.

Governance over IT in the Federal space has been an issue for many years and to date has not been solved. FISMA, which was enacted in late 2002, was a start in attempting to set up roles and responsibilities, including defining the roles of Federal CIOs and CISOs enabling security structures to be built in Federal Executive branch departments and agencies, as well as establishing reporting process for incidents to US–CERT. This all being said, there were overarching and important components of a success risk management strategy that have been missing. As it stands today, the only requirement a Federal department or agency has is to report the incident to US–CERT in the dictated time frame based upon incident categorization using a 20-year-old taxonomy that no longer describes the types of attacks that organizations are experiencing. This creates inaccurate metrics, and little to no real data on the actual attacks that are occurring in the Federal civil space. US–CERT does not have the authority to require the departments or agencies to share detailed information, or follow any specific instructions. Departments and agencies interpret their reporting requirements differently and therefore each reports incidents using different definitions and methodologies. When I was the Director of US–CERT if we needed Federal departments and agencies to follow specific instructions, we would have to have the Office of Management and Budget (OMB) require them to follow the instructions. Despite even OMB guidance, the cooperation from Federal civilian agencies was consistently on the low end.

Because many of the existing IT systems are owned and operated by Federal departments and agencies, there is no existing direct authority for DHS to require cooperation with US–CERT. This being said, it should also be understood that some of the departments and agencies have more sophisticated operations than US–CERT. The security operations centers at State Department, Department of Justice, the Federal Aviation Administration have a much higher technical monitoring and response capability than US–CERT. In order for US–CERT to accomplish the mission of protecting the Federal civilian agencies and departments day in and day out, US–CERT must be empowered and its capabilities must continue to be developed. It must have a clearly defined mission, authority, and budget. It must have tools. These tools must be determined by what will support the mission, not be tied to legacy systems, management, or contractors. This must be a collaborative mission between US–CERT and the departments and agencies. A "dictatorship" is not what is needed. Collaboration and cooperation will enable the road to success. Even more important is to clearly define US–CERT's role and the authorities the organization and Director carry. Developing a "council" of Federal department and agency Security Operations Center Directors and the Director of US–CERT to help guide this mission makes sense in order to ensure the mission of US–CERT stays on track, serves its Government customers, and has a focused and effective mission strategy.

Today US–CERT is buried too deep within DHS. To even confuse the issue more, US–CERT is a part of the National Cybersecurity and Communications Integration Center. Instead of integrating the NCC into US–CERT, yet another functional area has been opened, creating and compounding the confusion. US–CERT must be given autonomy to allow it to function as a successful operational entity—not laden in the political quagmire of DHS, NPPD, CS&C, NCSD. In my view, in order to be successful, US–CERT should be removed from the National Cybersecurity Division (NCSD) and treated as a component organization similar to FEMA. It should have its own budget that is not constantly diluted by other, projects, programs and internal politics in NPPD, CS&C and NCSD. US–CERT should have a clearly defined mission with attainable goals and the autonomy to succeed in this operational mission. Yes, operational. This is a roll up your sleeves and respond mission. This mission cannot be performed anywhere else in the Federal civilian government . . . the White House cannot carry out an operational function, the DoD cannot perform an operational function of this nature domestically based on the Constitution, and no other department or agency has the overarching mission that allows for both emergency

response and homeland protection. DHS makes functional sense; US–CERT must be empowered to fulfill its operational mission. As it stands today, US–CERT is constantly caught up in political priorities and much time is spent thrashing around, attempting to service too many projects and stakeholders. A clear governance process in the Federal space, a clearly defined mission and the authorities to support that mission, a budget to carry out this operational mission, as well as autonomy to operationally perform the operational duties are the steps to US–CERT having the capability to make a difference in supporting the departments and agencies as a part of DHS.

US–CERT's other mission is to coordinate and collaborate with the private sector—specifically with critical infrastructure owners and operators—is equally as important. Again, great mission, but rarely accomplished. The work is often clouded by poorly defined expectations and internal politics. US–CERT has absolutely no authority within critical infrastructure that is owned or operated by the private sector—nor should it. The Federal Government has no claims or authority over privately held companies. Even in some of the current draft legislation in both the House and Senate, participation in Government-led cyber activities is by invitation only. Today's private-public partnership efforts are bogged down with the same rhetoric, politics, and legal barriers of the past 20 years. I will say that presently US–CERT does little of the coordination. This is done primarily through NCSD. Most of the communications is done by the CSCSWG (Cross Sector Cybersecurity Working Group, a working group of the ISACs) and most of the members are not actual security professionals running security organizations, but a confusing mix of IT and communications companies with individual company-focused agendas and little or no focus on the operational agenda. An operational unit like US–CERT must be firewalled away from this kind of dysfunction to allow it to concentrate on the operation response mission.

The relationship between US–CERT and the private sector must be a focused and well-defined mission. Prioritizing work with the infrastructure providers—not individual IT product vendors—such as ISPs, web hosting and caching, cloud providers and IT infrastructure providers—to enable the focus on the operational response mission. I understand the entire private sector IT and communications sector wants to participate in future policy creation, but that function must not be mixed with the operational mission US–CERT must succeed in.

So far, I haven't painted a very pretty picture of what is going on at DHS in regards to cyber, but I want to re-iterate that I do believe DHS is the right place for cyber. I also believe changes need to be made in order for DHS to have a successful cyber mission. Giving US–CERT the autonomy to embrace a well-defined operational response mission (both with the departments and agencies as well as with critical private sector players), with a budget and capabilities to execute on the mission, and authorities to enable them to execute on the mission is a very important step to success.

Creating a successful public-private partnership to help secure cyber space is yet another mission that must be addressed. I think we need to approach this problem from a different direction. We must not look at it as a "cyber space" problem. That mission space is far too broad. We must look at this problem in digestible pieces. Internet infrastructure: Internet Service Providers, Cloud Providers, Web Providers and Information Infrastructure Providers. Separate this from the "cyber war" issue, separate this from the policy and legislative issues. Move these layers away from the operational mission of US–CERT. Take on the protect the infrastructure problem first. Work on the information sharing problem with an operational lens. I truly believe a technical solution must come in order to break the stalemate we find ourselves in with regards to cooperation and information sharing. The stalemate is centered on procurement, legal, privacy and proprietary information issues. We must determine a technical function for anonymously exchanging information. In addition, we must start articulating the problem with the same vernacular. We must spend time redefining the taxonomy and vernacular we use to work the cyber problem. We must do this in order to establish meaningful metrics, solutions, and focused solutions to the problem.

The ancient category one through eight taxonomy, where 99% of all incidents are categorized as category three "malware"—is useless in the world of complex attacks and sophisticated adversaries. I do believe this will become easier as we move on our continuum to the cloud. I believe as it becomes a more defined industry and who actually runs the "IT infrastructures" (i.e. clouds) becomes more defined, information sharing will become better as a function of how many entities must actually participate in the defense of IT as a whole. It must be understood that a public-private relationship is a two-way street. Often the Government is left holding the bag of failure when it comes to this relationship. The burden here is not and should

not be solely on the Government. We all have critical information that, if shared, would help the community as a whole. In the near future, the Government will be squarely in the customer role as we move on the IT continuum to the Cloud. We must look at how the Government and private sector can shape a healthy relationship. I am a firm believer that the private sector needs a private non-profit entity that would facilitate the relationships of the many privately held IT companies. This non-profit entity would facilitate the information sharing both on the private side as well as a focused conduit for information sharing with the Government. I do not see this as an inherent Government-only role. I clearly understand there is a National defense role for the Government in times of war, but we need to clearly define what that means in terms of cyber, and yes that is clearly a DoD role—not a civil Government role.

This being said, I do see technology developments that will remove the legal and privacy issues around information sharing. We must technologically come to a place where we can exchange information on a technical level about threats, attacks, and mitigations without disclosing information about the entity or entities involved. We must focus as a community—not as a Government—on moving this solution track along. We must be mindful of the circular rhetoric trap we get caught in when we hear the words—public-private partnership—and realize the actual work that needs to happen to accomplish the goal—defending our IT assets and missions. The work that needs to be done is to create technical processes, overcome procurement and legal issues. This must be done as a community, lead by the private sector. The Government's participation should be as a member of the community.

In conclusion, I do believe DHS has a primary role in cyber. Though I have not always thought DHS could handle the important mission because of its maturation level, I do believe the operational mission of US–CERT belongs in DHS—but as an autonomous operational component with direct reporting capabilities to the Secretary. I believe the mission of US–CERT must be more clearly defined to enable it to be successful. The appropriate authorities must be given to US–CERT to allow it to function. Public-private partnerships need to be rescued from the circling drain of rhetoric and lead by the private sector with Government participation.

We are moving rapidly to a new world—we must clear our plates of the static yada yada of stale circular discussions, identify the operational function and technical solutions. Empower US–CERT to succeed. Empower the private sector to lead. Empower the Government to participate.

Thank you for this opportunity to testify. I would be happy to answer any questions you may have at this time.

Mr. LUNGREN. I thank you all for your testimony.

I thank you all for being cognizant of our time limits, and I appreciate that.

Dr. Schneck, how do we solve this problem of stronger protections for sharing information from the private sector to the Government? The reason I say that is, you have members of the public who are naturally suspicious or skeptical of the Government working with the private sector and not protecting the individual rights of consumers and so forth.

If I am a credit card holder and all of a sudden, I find that my credit card has been cancelled through no action of my own, which happened one time when I tried to present it at a restaurant, and then 2 days later, after we called one of the major credit—that night when we tried to call them—well, first of all, my wife went on the internet to find out what our account was, and our account was gone. Then they told us, well, they would send us a card in a couple of days. Now, obviously there had been some sort of a loss of security within their operation, but they didn't tell me what it was all about.

I suppose, so long as I didn't suffer anything beyond that—however, if I had been traveling in the middle of the country and only had one credit card, I would have been in real trouble. But they obviously didn't want to share with me whatever that was; they believe that they took care of it internally.

But members of the public might be a little skeptical if there is this broad protection that no matter what the company involved with that information did, as long as they shared it with the Government, they were protected from any liability, on the one hand.

On the other hand, we want companies to come forward with information about how there has been an intrusion. We want that shared.

Where do we strike that balance? How do we strike that balance from your point of view?

Ms. SCHNECK. So, thank you, Chairman Lungren, I will start out by saying I am not a lawyer. I surround myself with a lot and actually find it fun.

Mr. LUNGREN. Well, we have an abundance of lawyers here, so we need some help.

Ms. SCHNECK. So, first, on the note of your lost account, it likely is somewhere in Romania, and we can help with that later.

The issue is difficult at best from what we see. You said the word that I would choose, and that is balance. So, first and foremost, we are not talking about sharing any kind of PII or private information.

This type of data looks at volumes of traffic, malicious code, malicious code that we can say, at a human level and at a machine level for a lot of math, looks the same for a variety of parameters. One might be an encryption algorithm that is not commonly used, but, look, it is used here and it was used here on the other side of the planet within the same 2 hours from machines that have the same pattern of sending traffic.

That is the kind of data that our analysts and we call our colleagues within the sector and across the critical infrastructure sectors, and we reach out to the US–CERT. We reach out to the FBI National Cyber Investigative Joint Task Force with this kind of data of, and then it builds into a much bigger picture.

The analogy I would use is from my days working as an intern in a weather lab. If you see a lot of cold air above a lot of hot air with wind direction in the opposite waves at certain levels from the altitudes and then an air pressure that is fairly low over a large region, any one of those things could mean just a little storm. But if you put those together, and you have a tornado, high probability.

What we want to share is not the air temperature in every county; what we want to share is the people that need to leave their homes, and we need to be able to do that more quickly. So there is a big picture that we draw.

The problem is when you share out that big picture, such as XYZ is happening in this sector, are we endangering the companies in those sectors that we have already protected, both electronically as well as informing the humans in those companies, do we risk them having material shareholder issues? This is such a new area for policy. That is the problem.

Mr. LUNGREN. Well, I would love to work with you and any lawyers that you might run into on that, because I do think that we have to have a greater accessibility of information in both directions, and sometimes liability issues will interfere.

Let me ask you this. You used a great analogy, you said vaccination doesn't work any more. Golly, I have McAfee on my computer,

and I thought I had vaccinated myself against intrusions. Now you are telling me that my attempt at vaccinating myself, my computer system, isn't enough?

Ms. SCHNECK. First of all, any security provider that says you are 100 percent safe, I would get rid of them.

Mr. LUNGREN. Well, McAfee has never told me that.

Ms. SCHNECK. All right. So, second, you are vaccinated against everything that we in the community know about.

The problem is the bad guy creates this code that changes itself, just like the flu mutates, so we worry about the new vaccine, in case your body can't deal with the mutation of the disease and you get sick anyway.

What you are protected by with McAfee is the view of the whole world now, so not just what we know about but what we are seeing happening right now. Believe it or not, you are able to be protected against something that might have been developed on the other side of the planet that comes in with a risk score so high it may not have a name, but you are going to block it.

That is the new paradigm we need, and it is not just our data. We need the ability to combine our data with data from other sectors, across the energy sector. What is the energy sector seeing in cyber?

As a vision for the future, to Mischel's point, it will look a lot different and a lot better in the future and we can leverage the power of the cloud that was mentioned by being able to put this kind of data together, infuse it into the fabric, and make things more intelligent.

Mr. LUNGREN. Thank you.

My time has expired.

The gentlelady from New York is recognized for 5 minutes.

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

Ms. Kwon, cyber intrusions affect the private sector even more than Government networks. Some of these private networks involve critical infrastructures necessary for our society and our economy to function.

What can DHS do to foster better cybersecurity practices in the private sector? Does DHS need regulatory or enforcement authority for critical infrastructure sectors, and should the private sector be doing more on its own? If so, why isn't it happening?

Ms. KWON. Well, this has been always the very difficult question because our critical infrastructure is not owned or operated by the Government. Therefore, the Government does not have any authority over the private sector.

What is needed here is better collaboration and better communication.

Whether regulation is needed or not, I am not a regulator. I am not in that kind of business. I am a technical geek by nature. So I will leave that decision to the lawmakers and the regulators.

But enabling us to more clearly communicate amongst the Government and the private sector and share that critical threat information is actually—is very important. But even more than that, DHS helping the security teams that work in those critical infrastructure environments to communicate with their executives and their board members to enable the financing that needs to be put

behind securing critical infrastructure is critical and important and to helping them accomplish their mission.

Mr. LEWIS. Can I just jump in on that one for a second? We did a poll with McAfee recently, and it found that two-thirds of the electrical companies in the United States had found Stuxnet on their system, two-thirds. Of those two-thirds, only 40 percent had taken steps to remove it.

Does that make you feel good? Not me.

I think if we don't give DHS more authority, we will not succeed at this, and I think CFATS might be a useful model to think about.

Ms. CLARKE. Thank you.

Dr. Schneck, your recent report on Chinese-sponsored hacking into our energy sector computers was very concerning. Is the industry now fully aware of this issue, and if so, have you seen evidence that they have acted to protect themselves? If not, why not, and where is the disconnect?

Ms. SCHNECK. So, on the question of, is the industry fully aware, from reports like these that we have done with CSIS, we consistently get surprise answers back. So, for example, security spending last year went down with the recession, even though awareness of the threat went up. So awareness and acting may not always be related.

In addition, when you talk about being aware, although many are aware there is a threat, I think that both public and private can do a better job of explaining what that threat really means. For example, you can have, you can have the malicious code on your system, and it wouldn't be a threat, and there are two cases why this is true.

One is, if you are not running any systems that that code can actually access or use to your harm, you don't need to worry about that particular threat, so we need to do some risk analysis, back to the comment earlier about looking to the CFOs and the risk people in each company; this is all a question of the risk.

But the second thing is there is technology today that can sit very quietly on a system and just decide these X processes may run, that is it. Anything outside of those processes simply should not run. So we are working with our colleagues and our partners on how you embed this kind of technology into the big component levels of industrial control systems, because we can't always assume everyone is aware. This rose so quickly, we can't make everyone aware, and we certainly can't predict the next threat as quickly as the bad guy can send it.

You are leveraging the power of light. This is happening in bits and bytes at the speed of light. So what we can do is say, only those authorized can act.

Ms. CLARKE. Thank you.

Mr. Lewis, in your writings, you have talked a lot about public-private partnerships for the cybersecurity mission. Can you explain to us what roles you feel each side needs to play? What, for example, are the inherently Government functions, the public side, and what components are best left for or even must be left for the private sector?

Mr. LEWIS. Thanks. That is a great question. The obvious place to start for me is that development of technology has to be left to

the private sector, and they are just the masters at it. We have to let them do it.

A place where public-private partnership makes sense is on information sharing, and it is easy to get sort-of distracted by the numbers in information sharing, but basically, there is a small set of companies that have, including McAfee and Symantec and others, the big telco operators, the big ISPs like Comcast or Cox, put them together with DHS and with NSA, and we will have a pretty complete picture of what is going on, on the internet.

Now there are legal impediments to doing that, right, and that is a harm to the ability to secure our Nation's networks. But that kind of focused information sharing with a small group of companies is a perfect place for a public-private partnership.

On the other hand, there are some threats that only the government can deal with. If we are talking about the Russian military or the German military or al-Qaeda or the Iranian and North Korean military, that is a government response, and there is no company—the story I like to show is Google, greatest technology company in the world, some would say, didn't take the Chinese very long to get through their defenses. There are some things only government can do.

Mr. LUNGREN. The gentleman from the second-largest State in the union, Mr. McCaul, is recognized.

Mr. MCCAUL. California is close behind, I might add.

Jim, it is great to see you again.

Dr. Schneck, thank you for your service on the commission as well.

I assure the Chairman that I was not personally responsible for the 40,000 downloads of that report, but I will, I just want to commend your leadership, which was far greater than mine, in really herding cats on some of the top experts in the Nation, putting that report together. Perhaps we should call you the bots herder in cyber terms, I don't know.

You know, 15,000 Federal intrusions take place per day, so you are going to have 40,000 downloads over a period of a year or so, but 15,000 intrusions per day on the Federal Government. As was pointed out, the three levels we always talk about is the criminal aspect, the espionage and the warfare piece.

God knows how many are taking place in the private sector. I am sure it is far greater than that. When you look at the amount of data that has been stolen from just the Federal Government alone, it rivals the Library of Congress, so it is a very serious issue.

Jim, I just want to throw out just a very generic question. Since the time of the report, I think the threat level has increased. Do you feel that we have made any progress, and do you feel that in any way we are safer?

Mr. LEWIS. Thank you, and I do want to say that I believe Congressman McCaul is right in that there were lots of clicking noises late at night from both of our offices, but that wasn't the cause of the downloads. So are we making progress? The answer, I think, is, "Depends."

When you look at the Department of Defense, some tremendous efforts with the creation of Cyber Command. When you look at the Department of Homeland Security, significant improvement. I

think you heard Phil describe that. Other departments, State, Commerce, have made some efforts.

So, overall as a Nation, OMB with its efforts to revise FISMA and to find a better way to secure Federal systems, those are all signs of progress, but it is not enough. We were behind when we started, as you know, and we have not caught up.

So do I feel like we were more secure? We were on the path to being more secure, and I think the work that this committee and others in Congress can do might get us there by 2012, but we are not there yet.

Mr. MCCAUL. With respect to—I am sorry, Ms. Kwon.

Ms. KWON. Yes. I just want to add something to that in that we do spend a lot of time talking about the success of DHS, but I also want to say that there has been a lot of great success among the departments and agencies. They have, over the past several years, stood up several security operation centers and have improved the security amongst some of the larger departments and agencies, and I think that needs to be recognized.

I think a lot of that comes from the actual awareness that has been brought to bear through the CSIS Commission and other efforts in getting the word out that cyber needs to be a priority.

But I do think, in looking towards the future and things that we need to improve is improving that communication within the Government on the Federal, civil, civilian side of the house, getting DHS to work more closely, not only with private sector but with the civil agencies, CIOs and CISOs and work that improvement across the Federal space together.

Mr. MCCAUL. One thing I noticed both you, Ms. Kwon, and Jim mentioned was that DHS needs more authorities and that you, I think you mentioned appropriate authorities must be given to US–CERT. Can you be more specific?

Ms. KWON. Well US–CERT does not—the authorities US–CERT has today are centered around what they have with FISMA and the reporting that the departments and agencies must do with them.

The problem with that is reporting is simply reporting, working together is not working together.

So being able to work from a position of authority during an incident with the departments and agencies, to request information from them, to have certain actions performed, it is very important for them to have that authority over the space they are trying to protect, and they don't have that authority today.

But in giving them the authority, they also have to have the relationship with those departments and agencies. I think that is where we are falling short; we are talking a lot about authorities and more of a dictatorship and what we really need to have is a collaborative partnership with those departments and agencies so that they can take the actions needed in the time of an event.

Mr. MCCAUL. I couldn't agree with you more on that.

You said something interesting that caught my attention that I hadn't heard before, and that is that the nonprofit could play a role in protecting the private sector.

Ms. KWON. Well, I often find that private sector also has a problem sharing with themselves. So sharing information about a cyber

attack is very difficult. I mean, it goes to reputation. It has financial implications. It can ruin and crush companies, as we have seen in the near recent past.

So it is important to be able to share. I think if we take the Government out of the picture and allow private sector to create a nonprofit together and start that sharing with the Government as being a member but not the leader, I think we might be able to find some success.

I also think that there are different levels of information that we are talking about here, whether we are talking about broad-threat information with attribution or whether we are talking about technical TTPs, ways in which the malware works, the actual code itself, how to detect it.

Being able to put together an organization that can share those very granular, technical bits of information I think is critical and important in moving forward and a way in which we can do it circumventing some of the problems of law.

Mr. MCCAUL. I wanted to ask a question about Einstein–3, but I see my time has expired.

Mr. LUNGREN. We might come back to you.

Mr. MCCAUL. Or somebody else. I would love a grade on Einstein–3. Maybe I will ask it in a written question.

Mr. LUNGREN. The gentleman from Louisiana, Mr. Richmond, is recognized for 5 minutes.

Mr. RICHMOND. Thank you, Mr. Chairman.

I guess this question is to Mr. Lewis. You were here when I was asking the question about the health, electronic health records and a baseline or a set of standards that we should have, and I am looking at part of your testimony where we talk about the smart grids and the voluntary approach.

I guess I am interested in your opinion on both with electronic health records and the small grid and how vulnerable we are, where we should be going and where we are today in light of where we should be.

Mr. LEWIS. Certainly. Thank you.

You know, a lot of times you will hear people say that we don't know what standards to put in place and there are too many standards or there are lots of standards, and that was probably true a few years ago.

But we are now at the point where between our ability to collect data, our ability to identify best practices, we can now start to do things. We can now start to think of standards or mandatory best practices that would improve cybersecurity, either in health or in smart grids, in the electrical sector.

So I think we are on the cusp of being able to make that leap. You can look at places like the Department of State that have put into place a set of standards that have been very effective.

In 2003, State lost 3 to 4 terabytes of information to an unknown foreign opponent who probably lived in China. Three or 4 terabytes is about the equivalent of a third of the Library of Congress. Today that couldn't happen because they have identified best practices and things you can do.

So I think we can say now, do this and we will be safer, right.

When it comes to actually putting those in place, HIPAA, very old, very prescriptive regulations have immense drawbacks, and we need to find a more flexible approach.

Smart grids, well, it will take a while before it's secure, that might be the nicest thing to say. It is not secure now.

People are trying hard, but as I think I mentioned in my written testimony, the process that the National Institute of Standards and Technology used was a consensus process of 475 members. One way to put that in perspective is that is about as many people as there are in the Congress. Suppose you had to get every single person in the Congress to agree to a rule. It would be a challenging exercise, and I think that is what is in front of us.

We can come up with standards. It is possible to say what works, but we don't have the processes in place to do that yet.

Mr. RICHMOND. Well, which is very long and especially when you talk about the smart grid, and now I think that my utility is starting to experiment with smart meters on homes. Is that just as vulnerable?

Mr. LEWIS. No, fortunately, because it means that an individual home or perhaps a block of homes would be more vulnerable, right, because the smart grid itself can be hacked. But it doesn't mean you will be able to hack the actual power-generating facility. It doesn't increase the vulnerability there.

So are you as an individual more vulnerable? Yes. But as a Nation, is our critical infrastructure more vulnerable? Not as much.

Mr. RICHMOND. It appears that in, I think it is just a given that we can accept is true, that this changes every minute, every second of every day, the risk assessment. I know, as a lawyer, the law changes a little less frequently, but we are required to do continuing education on changes in the law.

Is there an industry practice where the chief technology officer or whoever is responsible for threat assessments, do we have an industry standard or something where they stay up-to-date with the new threats, new technology, and as it comes abroad? I am sure McAfee probably has it; they do it on their own. But what I am thinking about, just smaller businesses, to make sure that they are aware of the seriousness of the threats.

Mr. LEWIS. I think we all want to talk on this one.

Ms. SCHNECK. So, thank you. I can speak for McAfee, and I can speak for the colleagues with whom we work. I will leverage a little bit of my experience.

A few years ago I ran, for about 8 years, the private-side sector of the FBI's InfraGard program. We grew that from 2,000 members to 33,000 members, bringing subject-matter experts across the critical infrastructure sectors into relationships with their Federal, State, and, most importantly, local community law enforcement officers and Government officials to share information about cyber and about all the sectors as they are all connected.

One of the things we learned very quickly is our small to medium business base, about 60 percent of our GDP, was probably the biggest beneficiary of these relationships because without that, they don't have the access and the resources that we are privileged to have in larger companies to educate our executives, to give our

executives the time to go out and learn what is really outside of your four walls.

I would recommend that, not just our organization but others, small to medium businesses, to your point, need to educate their executives on the crossover between the legal, the policy, and the technical because it really—they work together so much now. The point was made, a beautiful point earlier, about how we are now focusing on the chief financial officers and the risk officers.

When we need to tell a company not to sell something but to understand that there is a big risk, we go to the CEO or the CFO, so you will see law and policy, I believe, greater value placed on that and more effused used in our businesses' future.

Mr. RICHMOND. Thank you, Mr. Chairman. I yield back.

Mr. LUNGREN. The gentleman from Missouri, Mr. Long, is recognized for 5 minutes.

Mr. LONG. Thank you, Mr. Chairman. Mr. Lewis, I don't understand if I understood you right, were you talking about CFATS program when you said we should emulate that? CFATS, can you elaborate on that?

Mr. LEWIS. Sure, I think it was in Phil Reitinger's testimony as well. This is a program for the Department of Homeland Security that lets the Department set standards in cooperation with the operators and owners of chemical facilities for anti-terrorism purposes to make the chemical facilities more secure.

It is a little bit of a regulatory authority. It is a little bit of a partnership. CFATS is not a bad model, and there are things that need to be fixed in it, I think, and there are probably some issues on liability. But it is a way to say to the companies, here is our goal, you need to make your network secure and here are some hints, here are some suggestions on how you can do that. But you can do whatever you think is best to secure your networks. We have the ability to come in and look and say is it actually working.

So CFATS, not a perfect model, but it is a little more flexible than a heavy-handed regulatory approach, and it does seem to have had some success.

Mr. LONG. I, as a precautionary note, we had the folks from CFATS in a couple of weeks ago, and I asked them, after 4 years of their program and hundreds of millions of dollars, if they could name their top three accomplishments, things they had done. They said, well, Mr. Long, we would say, No. 1, we have identified the problem. So I didn't listen too hard to 2 and 3. So before we go dovetailing in and trying to emulate CFATS, I just want to make sure I understood which program you were talking about.

Dr. Schneck, I think that you kind of answered my question that I was going to ask you and on Mr. Richmond, however, I just wanted to for the record state that there is a small business in my district, a title company, that had $400,000 electronically removed, and we think, over the weekend, this is within the last 12 months, $400,000 removed from their bank account, and we believe, the authorities are telling us, that it ended up in Pakistan.

When we had Secretary Napolitano in, I was asking her about if the Secret Service is the one that is in charge of that. She didn't seem to think they were. The Secret Service had told us all please listen all along that they are. So I guess, is there any way small

businesses like that can protect themselves? So you did kind of cover part of it in Mr. Richmond's testimony.

Ms. SCHNECK. Absolutely. I think it is a good point to note also, and Ms. Kwon made this point earlier, there are many agencies that work together in this cyber endeavor. The FBI or the Secret Service, there are ways that they are interconnected. I think sometimes when we name one agency over another, we don't give enough credit to that point.

The Secret Service, not only part of DHS and their efforts, but they are an integral part of the National Cyber Investigative Joint Task Force, which I analogize a little bit to Noah's ark. There are one or two of each in that task force, so when we have a cyber investigation, we call them directly because I know that that data that we can share will get all across the agencies more quickly than if I make 20 phone calls.

So the Secret Service or the FBI, one may be working it at one point; the other organizations, like the US–CERT, the NCIC, everybody is engaged at that point.

There are things that small to medium businesses can do. My best advice from personal experience driving news programs at the local level as well, build those relationships before you need them. You can meet your State Homeland Security officers. You can meet your local police. You can meet—every FBI, every State has an FBI field office, some have more than one. Go in and meet, I would recommend, the cyber people, meet the Secret Service people that work there. They are all friendly, and they really do want that outreach.

DHS actually has a Protective Service Advisor Program, the CSAs. These are Federal employees that are positioned in each of our States. Some States, the bigger ones, have more than others. Their job, part of their job is to know the community, know the people there and know the mission of that State, and those are also great people and know they can tie you directly back to DHS.

The resources are there. I don't think we as a country have done enough to tell the smallest communities and the small to medium businesses that they are available.

Mr. LONG. Okay, thank you.

Ms. Kwon, for you, the large U.S. banks have tremendous security setups, and they still get hit, and if the largest U.S. banks can't defend themselves, how are regulations that we are going to impose, or what can we do to help the small businesses?

Ms. KWON. Well, this actually goes back to the question with Mr. Richmond and is a very difficult question because often implementing defensive security is expensive and often it is not affordable for a small business or even a medium-sized business, or in large corporations where large budget cuts have been seen over the past year, this is often a problem.

I do see the future of moving IT out of the individual organizations and into a hosted environment, into a cloud environment, is a good defensive mechanism for a lot of small companies. You are seeing a lot of that happening today, particularly in health care, as we are going to electronic health care records.

You are seeing a lot of doctors moving to IT services instead of hosting it in their own offices. That way the security costs can be

spread over many doctors' offices as opposed to being burdened with one. So I definitely see moving to new ways of implementing IT as a good solution for particularly small businesses.

Mr. LONG. Okay, thank you.

I yield back.

Mr. LUNGREN. I thank the gentleman for yielding back.

I thank the witnesses for your valuable testimony, both this panel and the previous panel. You have both help us very much as we are on this journey to ask the right questions and to come up with some of the right answers and to see what the proper role of the Federal Government is in this and where regulation is appropriate, where cooperation is appropriate.

I have also wondered where the insurance industry is appropriate in this, since they seem to have a record for risk management in the world, and how you join all those things together? Those are some of the things that we will be pursuing with this subcommittee.

Some Members of the committee may have additional questions for our witnesses, and I would ask you, if you would, to respond to those in writing. The hearing record will remain open for 10 days.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 11:55 a.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN DANIEL E. LUNGREN OF CALIFORNIA FOR PHILIP REITINGER

Question 1. The various drafts of comprehensive cyber legislation that have been circulating recently have attempted to re-organize the Department. In fact, the former Director of US–CERT states today in her written testimony that US–CERT should report directly to the Secretary.

Is this necessary?

What are the positives and negatives, as the Department sees them, to re-organization?

Answer. As detailed in the Quadrennial Homeland Security Review (QHSR), cybersecurity is a recognized and vital mission responsibility of the Department of Homeland Security (DHS). The United States Computer Emergency Readiness Team (US–CERT) is the operational component of the integrated capabilities within the Department to satisfy its cybersecurity responsibilities. US–CERT has an enhanced ability to keep DHS informed about important cybersecurity events since 2009. US–CERT provides watch, warning, and response functions through the National Cybersecurity and Communications Integration Center to the Government and to our international and private sector partners. The US–CERT provides daily input to the Secretary of Homeland Security. The current reporting arrangement has proven successful through CyberStorm III as well as all cyber events that have occurred over the past year.

Moreover, the QHSR was followed by the Bottom-Up Review (BUR), which included a plan for DHS to:

"*Increase the focus and integration of DHS's operational cybersecurity and infrastructure resilience activities.* DHS has substantial operational cybersecurity responsibilities, which are inextricably intertwined with its responsibilities to manage all hazards risk to critical infrastructure. DHS typically manages its operational responsibilities through operating components. However, the majority of DHS's operational activities relating to cybersecurity and infrastructure protection and resilience are currently administered by NPPD, which is designated as a DHS headquarters element. DHS will focus NPPD's activities on operations and more closely align cyber and critical infrastructure protection and resilience efforts, in cooperation with the private sector, to secure cyber networks and make critical infrastructure resilient."

Thus, DHS is moving to increasingly integrate physical and cybersecurity operations across critical infrastructure. Isolating US–CERT from that integration could degrade the Department's ability to respond to complex incidents.

Question 2. You mentioned in your statement that DHS signed an MOU with DoD that "aligns and enhances America's capabilities to protect against threats to our critical civilian and military computer systems and networks." How does this MOU benefit the private sector, if at all?

Answer. The Department of Defense (DOD) and the Department of Homeland Security (DHS) already work closely together, and this agreement formalizes a process to increase the ability of each agency to work in its mission space. In particular, DHS leverages DOD's significant technical capabilities through its National Security Agency (NSA). To support DHS activities in protecting Government civilian networks and critical infrastructure, DOD has collocated a Cryptologic Services Group and a Cyber Support Element at DHS's National Cybersecurity and Communications Integration Center (NCCIC), the hub for responding to domestic cyber incidents.

Through enhanced joint planning and better visibility into each others' operational processes, the Memorandum of Agreement (MOA) will increase each agency's effectiveness and build on the capabilities of each. This in turn will enhance the re-

sponse capabilities of both agencies while dealing with incidents that may affect the private sector.

The MOA does not alter existing DOD and DHS authorities, command relationships, or other oversight relationships. The MOA will not extend DOD's cyber involvement with the private sector beyond its current role. DOD already operates within DHS's National Infrastructure Protection Plan (NIPP) framework as the Sector Specific Agency for the Defense Industrial Base. Within the critical infrastructure and key resources community, DOD works directly with defense industrial base partners, DHS and Sector Specific Agencies (SSA), and other critical infrastructure partners in developing plans to assist in reducing risk and better securing critical infrastructure information systems.

Moreover, the MOA provides a framework that enables DHS to fuse DOD and NSA information, through the NCCIC, with that of the private sector. This provides all parties with a more comprehensive situational awareness of cyber activity impacting the Nation, and permits all parties to respond more effectively to those threats.

Question 3. How has the OMB memo providing DHS with operational review of Federal CIO's compliance with FISMA going to affect the cybersecurity program within NPPD?

Will taking on such wide responsibilities alter the priorities within the cybersecurity mission? How will the cyber mission be affected?

Answer. Office of Management and Budget (OMB) Memorandum M–10–28 "outlines and clarifies the respective responsibilities and activities of OMB, the Cybersecurity Coordinator, and the Department of Homeland Security (DHS), in particular with respect to the Federal Government's implementation of the Federal Information Security Management Act of 2002 (FISMA)." It assigns DHS immediate primary responsibility for the operational aspects of Federal agency cybersecurity with respect to FISMA, including, but not limited to:

1. Overseeing the Government-wide and agency-specific implementation of and reporting on cybersecurity policies and guidance;
2. Overseeing and assisting Government-wide and agency-specific efforts to provide adequate, risk-based and cost-effective cybersecurity;
3. Overseeing the agencies' compliance with FISMA and developing analyses for OMB to assist in the development of the FISMA annual report;
4. Overseeing the agencies' cybersecurity operations and incident response and providing appropriate assistance; and,
5. Annually reviewing the agencies' cybersecurity programs.

The memorandum enables new, proactive protection activities, which complement the Department's pre-existing, reactive incident response activities in the area of Federal Executive branch agency cybersecurity. While the United States Computer Emergency Readiness Team (US–CERT) is already focused on detecting malicious activity and providing incident response support, the new activities permit DHS to better understand the Federal Executive branch's cybersecurity posture from both an agency-specific perspective and on an enterprise-wide basis. Examples of specific activities include: FISMA reporting to OMB based on agency periodic reporting through the CyberScope platform; recurring Cybersecurity Compliance Validation (CCV) program engagements with agencies; and establishment of Government or private sector Shared Service Centers (SSCs) and Blanket Purchase Agreements (BPAs) that deliver cost-effective security solutions to Federal agencies and further permit those agencies to allocate limited resources to more mission-critical activities.

As it continues to implement the memorandum, DHS will conduct annual agency Chief Information Officer (CIO)/Chief Information Security Officer (CISO) interviews to maintain awareness of agency-specific successes and challenges. Interview input enables DHS to better assess Government-wide and agency-specific needs and gaps, which ultimately leads to establishing new, targeted capabilities or processes. DHS recently also began conducting CyberStat reviews with Agency CIOs and CISOs in coordination with the National Security Staff and OMB to assist agencies in defining action plans to improve FISMA-related cybersecurity capabilities.

Undertaken by the Federal Network Security (FNS) branch within DHS' National Cyber Security Division, the activities pursuant to the memorandum enable DHS and its agency partners to enhance their security posture before incidents occur. They also provide US–CERT with a clearer picture of an agency's networks, systems, and policies when investigating an incident and providing support.

Question 4. With regard to the private sector the Department is still more of a coordinator rather than a directive authority, is that an effective role?

Is the private sector being best served by DHS?

What additional authorities does the Department feel are necessary to better serve and protect the private sector, and especially critical infrastructure?

Answer. The Department of Homeland Security (DHS) has a clear authority to conduct analysis, develop mitigation plans, and provide warnings with regards to cybersecurity. DHS serves the private sector in these capacities on a daily basis. However, nearly all of our private sector programs are built on voluntary participation. These programs have provided valuable, timely, and actionable vulnerability information, risk assessments, and mitigation strategies to our private sector partners.

For instance, both the Cyber Security Evaluations Program and the Control Systems Security Program (CSSP) conducted more than 50 on-site voluntary assessments in fiscal year 2010. Within CSSP, the Industrial Control Systems Cyber Emergency Response Team (ICS–CERT) provides on-site support to owners and operators of critical infrastructure for protection against and response to cyber threats, including incident response, forensic analysis, and site assessments. ICS–CERT also provides tools and training to increase stakeholder awareness of evolving threats to industrial control systems. The United States Computer Emergency Readiness Team (US–CERT) also provides similar vulnerability, assessment, and mitigation information for private sector business networks, upon request. Similarly, a large number of private sector participants take part in the Cyber Exercise Program, including the recent Cyber Storm III. These exercises are designed to increase the preparedness of individual participants, and across the public-private response community as a whole.

Question 5. What is the goal 10–15 years down the road for dot-gov protection?

Answer. Dot-gov protection is a complex, multi-enterprise issue. The challenge for dot-gov protection increases as the complexity of the Information Technology (IT) environment and the data and services consumed become more distributed. The technologies used to manage information and to create services that defend information must evolve with the larger environment.

Dot-gov protection must transition from network and signature-based security to security that also incorporates information and user-centric security. Government must adopt IT innovations that better serve Federal dot-gov users and the users who interface with Government systems. To effect this transition, Government must make fundamental changes in the following areas:

Security Operations

Coordinated Risk Management.—Policy and standards must build on knowledge and experience drawn from various sources, including intelligence, law enforcement, industry, Government departments and agencies (D/As), and others. The Federal Government will continue to play a significant role in the development of policy, standards, and countermeasures.

Information Sharing.—Information sharing that ensures the rights, privacy, and protection of individuals and their information is critical—particularly with the continued expansion of cloud computing, solutions as a service, and social networking.

Distributed Execution.—Distributed execution requires increased partnership with D/As and industry. D/As must continuously monitor their networks and hosts in order to provide insight into the health and status of Federal systems. Government relies on industry to: (1) Build product capabilities that secure customers, (2) develop system capabilities to provide increased capability to self-heal, and (3) provide prevention-oriented solutions to seek out, detect, and protect the user from malicious actors.

Technology Attributes

Identity Awareness.—Full protection of dot-gov requires development of "identity awareness," which is a capability that provides every component in the "service chain" with the ability to validate identity, ensure its authenticity, and provide access based on the role of that identity.

Agility.—Advances in mobile computing, cloud-based systems, and telework are posing new security challenges to the traditional concept of a static security perimeter protecting private Government systems and information. Government must be able to adapt as Government information is stored and accessed wherever an agency mission requires it. The security challenge associated with this agility is deciding which new risks are, or are not, acceptable when operating in a dynamic, mobile, and cloud-based computing environment, which may be only partially under the agency's control.

Diversity.—In the past, Government agencies operated relatively homogenous computing environments; Intel-based workstations running Microsoft operating systems were the norm. Now, we see a proliferation of device types (netbooks, smartphones, and tablets) joining traditional workstations and laptops. The industry development cycle is now measured in months. We can't predict the next great device or program, however, we know the trend runs towards smaller, more capable, and

cheaper devices. Furthermore, capabilities begin to blur as new generations of devices emerge. For example, we now judge phones on their ability to run applications and computers on their ability to make calls. The security challenges associated with this diversity of devices ultimately impacts our ability to secure these devices without degrading their capabilities.

Convergence.—As device diversity grows, we begin to see a convergence in network space and functionality. Accessing dot-gov no longer requires a user to sit in front of a computer. They may access our networks from any type of network, including traditional Ethernet, telephone systems, cellular lines, or wireless networks. Gone are the days when we could devise protections based on relatively stable, predicable network paths. The security challenge associated with this convergence ultimately concerns our ability to secure these pathways without disrupting connectivity.

In order to address these changes, Government must partner with the private sector and academia to develop new security ideas. These new ideas must be based on an information- and user-centric view that enhances new capabilities, rather than impeding them. These considerations are among those addressed in *Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action.* This paper, recently published by DHS, presents a five-level maturity model for ecosystem focus and convergence that is associated with increasing agility and provides an approach for achieving and employing these various levels. Ecosystem maturity is further explored through a discussion of healthy attributes.

Source: *http://blog.dhs.gov/2011/03/enabling-distributed-security-in.html*.

Question 6. Are private sector entities responsive to the efforts the Government makes with them to warn of threats and mitigate the consequences of attacks?

Answer. Due to the variety of Department of Homeland Security (DHS) programs and activities engaged in collaboratively improving cybersecurity, and the diverse nature of the private sector, private sector responsiveness varies considerably. Several examples of private sector responsiveness are outlined below.

United States Computer Emergency Readiness Team (US–CERT).—Formed in 2003, US–CERT is the operational arm of DHS' National Cyber Security Division. US–CERT's mission is to lead and direct efforts to improve the Nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the Constitutional rights of Americans.

If a private-sector entity requests assistance from the Government, DHS may provide on-site or remote assistance to perform analysis and recommend mitigation actions through US–CERT. This assistance, which is based on a signed request for technical assistance, is designed to assist private sector entities in detecting the scope of the malicious activity and determining mitigation actions to protect the system from current and future attacks or breaches. In addition, US–CERT provides standardized warning and mitigation information products to its private sector partners and constituents through its secure portal and through its public facing website.

The private sector's response varies depending on the entity and circumstances. However, we have seen growing private sector interest in receiving DHS on-site or remote analytical support. Some issues that may inhibit private sector responsiveness include concerns about: (1) Exposure of proprietary data; (2) prosecution or regulatory action; and (3) negative publicity.

Cyber Security Evaluations Program.—Since 2009, the National Cyber Security Division's (NCSD) Cyber Security Evaluations Program has conducted on-site assessments through its Cyber Resilience Review. In 2010, NCSD deployed its first Cyber Security Advisor (CSA), located in the mid-Atlantic region, to promote cyber preparedness, risk mitigation, and incident response. In this short period of time, it has become apparent that many critical infrastructure owners and operators have a general awareness of cybersecurity issues, but only those partnering with fusion centers, the Federal Bureau of Investigation's (FBI) Infragard program, local communities-of-interest, or those that subscribed to the United States Computer Emergency Readiness Team (US–CERT) informational products, routinely receive Government-provided threat warnings. To date, only a limited set of owners and operators have been directly engaged in assessments or other targeted cybersecurity activities.

Private sector entities, however, respond well when the Government solicits their participation in specific initiatives and they readily work with the Government to identify appropriate subject matter experts within their organizations. They also work with DHS personnel and other Government representatives to develop threat mitigations. For example, recent Cyber Unified Coordination Group Integrated Management Team operations, under the National Cyber Incident Response Plan

(NCIRP), used joint private-public partnerships to raise alerts, and to focus subject matter expertise and create tractable risk mitigations.

Cyber Exercise Program.—Private sector partners repeatedly mention that Cyber Storm and other DHS-sponsored exercises help improve their individual and collective cybersecurity and incident response capabilities. The number of private sector organizations that played in Cyber Storm III represented a 75 percent increase over Cyber Storm II (from 40 to 70 participants). Private sector organizations also actively participated in initiatives resulting from Cyber Storm III, including development of the Cyber Storm III summary and observations report, making edits to the NCIRP, and continuing active membership in the Unified Coordination Group, an interagency and inter-organizational coordination body that incorporates public and private sector officials. Private sector organizations from three critical infrastructure sectors already have engaged with NCSD to conduct follow-on exercise activities that examine operational changes made as a result of Cyber Storm III.

Control Systems Security Program.—The private sector has shown growing interest in the services of the DHS Control Systems Security Program (CSSP), which works with public and private sector partners to improve cybersecurity of critical infrastructure industrial control systems. Since the advent of their activities, CSSP and the Industrial Control Systems Cyber Emergency Response Team (ICS–CERT) have grown in scope and received increasingly more requests for on-site incident response, assessments, control systems training, and other offerings. The statistical trend from year-to-year indicates that the community as a whole is showing an increased interest in the Government program. Their interest also serves as an indicator of the effectiveness of the program's outreach and awareness efforts.

More specifically, ICS–CERT works on a voluntary basis with critical infrastructure owner-operators to respond to and analyze control systems related incidents, vulnerabilities, and threats. The team can perform a comprehensive range of services and activities, including providing sophisticated analysis of malware and deploying full fly-away teams. ICS–CERT incident response teams (also known as fly-away teams), which are routinely requested by the private sector, deploy to critical infrastructure facilities bringing advanced and unique malware evaluation capabilities and leveraging our control systems expertise and fused intelligence analysis. The team then works with the company to develop and implement a mitigation plan to eliminate the malicious activity and limit the risk of future incidents. The team appropriately addresses sensitive information using Protected Critical Infrastructure Information (PCII) protections and works to mitigate any privacy and civil liberties issues. ICS–CERT is then able to carefully aggregate and anonymize data about the incident and disseminate early warning alerts and advisories to critical infrastructure owners and operators on a sector-by-sector basis. Actionable alerts to our stakeholder communities include threat information, validated vulnerabilities, and related patches and mitigation strategies.

Once the ICS–CERT actively engages with a specific private sector entity via the voluntary incident response process, oftentimes the company will continue to implement the mitigation solutions that are offered, and, if needed, request additional support from DHS in the area of control systems security. Quite often these engagements evolve into trusted long-term information-sharing relationships that benefit both the Government and the private sector.

In addition to sending fly-away teams, DHS is also able to proactively work with companies to conduct cybersecurity assessments using the Cyber Security Evaluation Tool (CSET). These no-cost assessments enable users to assess their network and ICS security practices against recognized industry and Government standards, guidelines, and practices. The assessment tool can be used independently by the asset owner, or upon request, CSSP teams can assist with a full assessment on-site. The completed CSET assessment provides a prioritized list of recommendations for increasing the cybersecurity posture of an organization's ICS or enterprise network and identifies what is needed to achieve the desired level of security within the specific standard(s) selected. The CSET has increased in popularity among our partners over the years; in 2010, for example, the CSSP conducted 50 on-site assessments spanning 12 critical infrastructure sectors (including the Electric subsector) and is on target to complete 75 in fiscal year 2011. The tool is now publicly available for download on the CSSP website, and countless copies of the CSET have already been handed out at conferences and other events.

CSSP also works closely with the Department of Energy Idaho National Laboratory (INL) to provide cybersecurity training to private sector employees. The training consists of a weeklong class held at INL, instructing in cyber protection and intrusion mitigation techniques. Response to the classes has been highly positive—thus far, DHS and Idaho National Labs have trained over 16,000 control system officials, from chief executive officers to technical operators.

DHS has worked closely with the private sector as it expands its diverse set of resources available to the private sector, including threat and vulnerability situational awareness, risk assessment, and mitigation, and remote and on-site assistance. The trusted relationships DHS has with the private sector—through engagements, working groups, co-location on the NCCIC operations floor, and outreach—have allowed DHS to incorporate private sector input at every step as we build our capabilities. Private sector engagement is a cornerstone of the Department's cybersecurity mission and we look forward to working with Congress to continue to improve private sector outreach efforts.

Question 7. How does the cloud, or computing as a service, change the cybersecurity mission?

Is the Department prepared for the Government's effort to move more and more computing resources to "the cloud"?

Answer. The cyber threat environment changes continuously as malicious actors adjust their tactics and adopt new technologies. Similarly, the evolution of network architectures necessitates a cybersecurity posture that is adaptable and focused on risk mitigation. Regardless of changes in network architecture, the Department of Homeland Security (DHS) will continue to execute its critical mission to create a safe and secure cyberspace.

Cloud computing, computing as a service, time-sharing, and utility computing raise many of the same security issues that emerged when shared computer services were created in the 1960's. Yet, the cybersecurity mission remains the same. The many advantages of cloud computing also create many security challenges. We can never eliminate all the risks inherent to cloud computing. Instead, we must accept that differing levels of acceptable risk will exist for different users. Even if private, community, and public cloud computing business models use the same security techniques and tools, different business models create different security risk environments.

DHS encourages cloud computing providers to propose innovative security solutions that effectively protect Federal systems, information, communications, and ultimately, the agency's mission.

DHS has avoided requiring providers to follow particular designs or architecture for cloud computing. For example, due to a constantly evolving threat environment, the Federal Risk and Authorization Management Program (FedRAMP) was established to provide a standard approach to assessing and authorizing cloud computing services and products. The National Cyber Security Division is actively participating in the FedRAMP development. FedRAMP allows joint authorizations and continuous security monitoring services for Government and commercial cloud computing systems intended for multi-agency use.

These considerations are among those addressed in *Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action.* This paper, recently published by DHS, presents a five-level maturity model for ecosystem focus and convergence that is associated with increasing agility and provides an approach for achieving and employing these various levels. Ecosystem maturity is further explored through a discussion of healthy attributes.

Source: *http://blog.dhs.gov/2011/03/enabling-distributed-security-in.html*.

QUESTIONS FROM CHAIRMAN DANIEL E. LUNGREN OF CALIFORNIA FOR GREGORY C. WILSHUSEN

Question 1a. In your testimony you comment how the Government is lacking a National cybersecurity strategy. I have three related questions for that issue:

How is the lack of a National cybersecurity strategy hindering the Government-wide cybersecurity mission?

Question 1b. How, in your opinion, is it hindering DHS's cybersecurity mission?

Question 1c. How is it affecting the private sector?

Answer. The lack of an updated National cybersecurity strategy can hinder the effective implementation of the Government-wide cybersecurity mission. Our work has demonstrated the importance of comprehensive strategies that specify overarching goals, subordinate objectives, supporting activities, roles, and responsibilities, and outcome-oriented performance metrics, as well as time frames to help ensure accountability and align agency activities with National priorities. National strategies help shape the policies, programs, priorities, resource allocations, and standards that can enable Federal agencies and other stakeholders to implement the strategies and achieve the intended results. Without such an updated comprehensive National strategy for cybersecurity, increased risk exists that our Nation will not be able to obtain the desired posture against sophisticated threats.

Our work has shown that Federal initiatives and efforts to improve information security have consistently fallen short of the mark. The following are illustrative examples:

- In October 2010, we reported that only 2 of the 24 recommendations in the President's May 2009 cyber policy review had been fully implemented. Officials from key agencies involved in these efforts attributed the partial implementation status of the remaining 22 recommendations in part to the fact that agencies had not been assigned roles and responsibilities with regard to recommendation implementation.[1] One of these recommendations was to develop an updated National cyber strategy; however, administration officials were unable to provide a draft strategy or milestones for when the updated strategy is to be finalized and issued. We concluded that Federal agencies appeared to be making progress toward implementing the recommendations, but lacked milestones, plans, and measures that are essential to ensuring successful recommendation implementation, including the development of an updated strategy. We recommended that the National Cybersecurity Coordinator (whose role was established as a result of the policy review) designate roles and responsibilities for each recommendation and develop milestones and plans, including measures to show agencies' progress and performance.
- Our examination of Federal efforts to address the global aspects of cyberspace determined that the U.S. Government had not documented a clear vision of how the international efforts of Federal entities, taken together, support overarching National goals and that the Federal Government had not forged a coherent and comprehensive strategy for cyberspace security and governance policy.[2] As a result, the United States is hindered in promoting our National interests in the realm of cyberspace. We recommended that, among other things, the National Cybersecurity Coordinator develop with other relevant entities a comprehensive U.S. global cyberspace strategy. The coordinator and his staff concurred with our recommendations.
- Our review of Federal cybersecurity research and development efforts found that among the most critical challenges was the lack of a prioritized National cybersecurity research and development agenda, which increased the risk that research and development efforts will not reflect National priorities, key decisions will be postponed, and Federal agencies will lack overall direction for their efforts.[3] We recommended several actions, including developing such a National cybersecurity research and development agenda. The White House Office of Science and Technology Policy agreed with our recommendation and provided details on planned actions.

The lack of an updated strategy can also affect the Department of Homeland Security's (DHS) and the private sector's cybersecurity efforts. While the existing strategy encourages action by private-sector owners and operators of cyber critical infrastructure, we testified in March 2009 that a panel of experts agreed that there were not adequate economic and other incentives (i.e., a value proposition) for greater investment and partnering in cybersecurity.[4] The panelists also stated that the Federal Government should provide valued services (such as offering useful threat or analysis and warning information) or incentives (such as grants or tax reductions) to encourage action by and effective partnerships with the private sector.

In addition, we reported in July 2010 that public sector stakeholders from DHS and other entities stated that improvements could be made to the public-private partnership, including improving private sector sharing of sensitive information.[5] We also reported that the expectations of private sector stakeholders were not being met by their Federal partners in areas related to sharing information about cyber-based threats to critical infrastructure. We concluded that the public-private partnership remained a key part of our Nation's efforts but without improvements in meeting public and private sector expectations, the partnership would remain less than optimal. As a result, increased risk existed that owners of critical infrastructure would not have the appropriate information and mechanisms to thwart sophis-

---

[1] GAO, *Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed,* GAO–11–24 (Washington, DC: Oct. 6, 2010).

[2] GAO, *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance,* GAO–10–606 (Washington, DC: July 2, 2010).

[3] GAO, *Cybersecurity: Key Challenges Need to Be Addressed to Improve Research and Development,* GAO–10–466 (Washington, DC: June 3, 2010).

[4] GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture,* GAO–09–432T (Washington, DC: Mar. 10, 2009).

[5] GAO, *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed,* GAO–10–628 (Washington, DC: July 15, 2010).

ticated cyber attacks that could have catastrophic effects on our Nation's cyber-reliant critical infrastructure. We recommended that the National Cybersecurity Coordinator and DHS work with their Federal and private sector partners to enhance information-sharing efforts, including leveraging a central focal point for sharing information among the private sector, civilian government, law enforcement, the military, and the intelligence community. DHS officials stated that they have made progress in addressing these recommendations; we will be determining the extent of that progress as part of our follow-up efforts.

Updating the National cybersecurity strategy can increase the likelihood of improving the cybersecurity posture of our Nation. Additionally, an updated strategy could help ensure accountability and align agency activities with the United States' long-term economic and National security interests, including globally promoting our National interests in the realm of cyberspace and ensuring that the Nation does not fall behind in cybersecurity and will be able to adequately protect its digital infrastructure. As the administration updates the current strategy, it needs to focus on clearly articulating goals and objectives, assigning roles and responsibilities, developing milestones, deploying sufficient resources, defining performance metrics, monitoring progress, and validating effectiveness of completed actions.

Our responses to these questions are based on previous work that was performed in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Should you or your office have any questions on the matters discussed in this letter, please contact me.

QUESTIONS FROM CHAIRMAN DANIEL E. LUNGREN OF CALIFORNIA FOR PHYLLIS SCHNECK

Question 1a. In your Although it's oft repeated, McAfee shared with us that when they discovered the Night Dragon attacks, those Federal agencies who were not contacted first, even maybe hours later, expressed their disapproval.

How do you coordinate sharing the information with the Federal Government?

Answer. We are committed to sharing threat information to help the U.S. Government gain a deeper insight into the threat landscape and respond to specific attacks. Toward this goal, we work closely with our customers to ensure that we adhere to our NDA's as required by the law. Once we are sure that we have met all of our obligations to our customers, we contact representatives in the various agencies with authority over cyber security. We do our best to contact all of the actors at the same time—whether in defense, civilian, or crime prevention institutions.

Question 1b. Does there need to be a single source of contact?

Answer. We believe that the information-sharing process is improving. A few years ago, we would experience, on a regular basis, a high degree of complexity and difficulty getting to all of the right decision makers in a timely way. We often found that agencies that had been briefed were unwilling to share information with their colleagues in other agencies. It generally took us 2 weeks to brief all of the officials in the agencies. More recently, we have found that the process is improving. During the recent Night Dragon event, we did one briefing, for instance, which included defense, NSA, and FBI officials. This was an example of an improved process.

We understand how complex the information-sharing challenge is in the U.S. Government. Many rules regulate the way in which information sharing is done, and there are limitations on the types of information various agencies can share with each other. These limitations derive from law and agency regulations that seek to balance National security, domestic security, and privacy rights. Nevertheless, we would urge that some type of enhanced procedure be put in place to facilitate the ability of companies to share information in a manner that enhances their ability to share information in a rapid and efficient manner with the Government. Remediating cyber attacks is a complex, time-consuming process and the more rapidly the private and the public sectors can respond, the sooner our teams can ensure that vital information and systems are protected from additional attacks. Bringing down the response time from weeks to a few days would do much to enhance the security posture of our country.

Question 2. In a briefing to staff, McAfee brought up the technique of "white listing" where a computer is essentially limited in what applications it could run, which could potentially limit malware from infecting a computer.

Could you give us a little more information about the technique and how you see it being used most effectively?

Answer. White listing technology ensures that only good executable code can run on protected systems. The technology is used to protect servers, endpoints, embedded devices, and mobile devices. It is used in many ATM's, point-of-sale terminals, and Supervisory Control and Data Acquisition (SCADA) systems. White listing technology narrows the scope of many embedded systems to ensure that an attacker can't install malicious code.

White listing is one of the exciting technologies of the future because it can enable organizations to be much more proactive in protecting their systems—it gives them much more control because only good communications can be received. This contrasts in a considerable way with the older model of security, the anti-virus model, which is inherently defensive. This model is based on blocking malicious code and letting everything else into customer sites. This model has been breaking down for some time given the geometric growth in malware over the last few years. McAfee detected as much new malware in 2010 as we detected since the founding of our company 19 years ago. White listing is an important part of the cyber security solution moving forward.

QUESTIONS FROM CHAIRMAN DANIEL E. LUNGREN OF CALIFORNIA FOR JAMES A. LEWIS

Question 1a. In some regulated industries, companies do only the minimum needed to stay compliant with the regulations. In the world of security, the minimum effort does not necessarily make one more secure.

How does one prevent the "race to the bottom" in a regulatory regime?

Question 1b. How do we change that culture of security to one not of mere compliance, but security?

Answer. Doing the minimum would be an improvement from where we are now. That said, there are several measures that can to prevent a "race to the bottom."

The first is to increase transparency and reporting on the number of probes, breaches, or service disruptions of computer networks. By reporting on the number of security failures, we would be able to assess the effectiveness of regulations. The larger goal is to move companies to automatic monitoring of networks and to adopt something like the "IT Dashboard" OMB is putting in place for Federal networks. The Security Content Automation Protocol (SCAP) NIST is developing is an example of emerging approaches that could automatic and accelerate cybersecurity efforts.

The second would be to allow for some kind of "spot checks" of computer systems, random checks to see if computer networks were adequately secured. This is a standard law enforcement and regulatory technique, and could involve DHS or some outside auditor inspecting the adequacy of a company's cybersecurity efforts. The knowledge that a random check could be carried out would in and of itself encourage better compliance.

A related goal would be to avoid defining compliance as a paper-driven process, where companies filed regular reports on performance. These are inadequate for several reasons, but the most important is frequency. Long annual written reports on compliance only benefit report writers. A better approach would be to require companies to immediately inform the appropriate agency when their networks have been successfully penetrated. This changes the metric for compliance. We want people to report failures and report the actions they have taken in response immediately. In this, a regulatory approach would be part of a larger effort to develop a broad understanding of the level and kind of malicious activities in cyberspace.

QUESTIONS FROM CHAIRMAN DANIEL E. LUNGREN OF CALIFORNIA FOR MISCHEL KWON

Question 1. In your written statement you advocate separating US–CERT, the operational arm, from the more policy- and coordination-driven NCSD. I'm interested in having you elaborate a bit more on that: How does separating elements of the cybersecurity mission benefit the Department and/or the private sector especially the critical infrastructure?

Answer. US–CERT is an operational unit with a very important mission to support the Federal departments and agencies.

(1) This mission is buried deep within DHS, which makes decision-making slow because of all the chains of command it must go through (NCSD, CS&C, NPPD). The operational mission is one that must be enabled to focus and act quickly.

(2) US–CERT is often distracted and taken off this mission by the policy and coordination arm of NCSD.

Cyber is a fast-moving space where nimbleness is important for success. It often takes US–CERT days, even weeks, to get approval for actions because of the need to go through NCSD, CS&S, NPPD, and then to get to the Secretaries' attention.

As issues go through this chain they are often distracted by politics and other priorities and delayed further, or veered off from the operationally correct decision. US–CERT is often volunteered for programs and projects by the policy and coordination arm, thereby taking it off its core mission and into projects that are not planned for, budgeted for, or in the scope of their expertise.

It is important for this operational mission to be clear. There must be firm process for changing this mission. It cannot be constantly changing and moving at the whim of politics driven by a policy team seeking its own success at the price of US–CERT's.

Today, US–CERT's clear mission—as stated in FISMA—is to support the Federal departments and agencies. If you were to ask the major departments and agencies how often US–CERT assists them, you will be surprised to find out that it is very little. US–CERT's focus is very fragmented and confused. It has been tasked by NCSD, CS&S, and NPPD to participate in a plethora of other projects that take US–CERT's understaffed, under budgeted, and technology-limited National security operations unit far away from its legislated mission space.

Question 2a. While you were with US–CERT, how often did you provide technical assistance to private sector entities?

Answer. Once. This is not US–CERT's mission, nor do they have the expertise, staff, or budget to assist the private sector on a regular basis.

Question 2b. Does the Department have an established process for private entities to request assistance?

Answer. No.

Question 2c. If so, how can it be improved? If not, what should it look like?

Answer. If US–CERT is to take on the mission of assisting private sector entities it would have to have an increase in budget, staffing, and tools. Currently, it is not their mission to assist private sector entities.

Question 3a. In your testimony, you stated that virtualization through "cloud" technologies is the future for information technology infrastructures.

What are the security risks of moving systems and applications to the "cloud"?

Answer. The security risks are similar to those of any IT infrastructure. The key here is that moving to the "cloud" is an opportunity to bake security in, build it more securely, and revitalize IT infrastructure and share in the cost of better security mechanisms.

Question 3b. Will we be more secure or less secure from cyber attacks?

Answer. It depends. If the opportunity to improve security is taken, it could be more secure, if not . . . no.

Question 3c. If the Federal Government and private companies are moving to the "cloud," what precautionary measures should be taken to maintain the integrity of these information systems?

Answer. First and foremost, we should be looking at new security technologies. Technologies where we can cleanse the known malware from the infrastructure layer. We need to move to technologies that allow us to understand what is good and what is bad. We need to move away from signature-based tools where we have to be infected first in order to detect the attack. We must move to a more defensive posture where the attacks can be detected and stopped on the infrastructure layer, before they reach the users.

Question 4a. In your testimony you discussed the stalemate of cooperation and information sharing with the private sector as a result of procurement, privacy, and proprietary information issues.

Answer. First it must be understood that most networks have already been compromised. It is actually the rare few who identify the intrusions. With this in mind, we must not take a position of punishment for those who identify the problems, but we must assist. We cannot allow cyber attacks to defeat our private or public sector entities.

Question 4b. What actions need to be taken to aggregate shared information about known cyber vulnerabilities from the private sector?

Answer. I'm not sure cyber vulnerabilities are the problem. We know about millions of vulnerabilities. We need to understand more about the attacks. As a community—whether we are private or public—we need to know more about the details of the attack that would enable detection. Not the "who", not the "what" was taken, but the TTPs, The Tactics, Techniques, and Procedures the attackers use. I believe, for both private and public, we need an autonomous entity (I referred to this in my testimony as a non-profit organization) that can take anonymous TTP information and make it available for others to use.

Question 4c. What other measures should be taken to encourage private sector's willingness to share information?

Answer. There are a few places where this can be improved for both private and public sectors.

(1) Take the attacks and the responses out of the public and press. You must take the reputational damage issue off the table.
(2) Lower the liability concerns.
(3) Have an anonymous way to share.

○