NAVAL POSTGRADUATE SCHOOL CENTER FOR HOMELAND DEFENSE AND SECURITY
HOMELAND SECURITY DIGITAL LIBRARY
SECURING THE HOMELAND THROUGH THE POWER OF INFORMATION

MARCH 13, 2013

DHS CYBERSECURITY: ROLES AND RESPONSIBILITIES TO PROTECT THE NATION'S CRITICAL INFRASTRUCTURE

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON HOMELAND SECURITY

ONE HUNDRED THIRTEENTH CONGRESS, FIRST SESSION

HEARING CONTENTS:

Webcast **[view video]**

Member Statements

Michael McCaul **[view PDF]**
Chairman
Committee on Homeland Security

Witnesses

Panel 1

Jane Holl Lute **[view PDF]**
Deputy Secretary
Department of Homeland Security

Panel 2

Anish B. Bhimani **[view PDF]**
Chairman
Financial Services Information Sharing and Analysis Center

This hearing compilation was prepared by the Homeland Security Digital Library, Naval Postgraduate School, Center for Homeland Defense and Security.

Gary W. Hayes **[view PDF]**
Chief Information Officer
Centerpoint Energy

Michelle Richardson **[view PDF]**
Legislative Counsel
American Civil Liberties Union

COMPILED FROM:

- *http://homeland.house.gov/hearing/dhs-cybersecurity-roles-and-responsibilities-protect-nations-critical-infrastructure*

Committee on
HOMELAND SECURITY
Chairman Michael McCaul

Opening Statement

March 13, 2013

Media Contacts: Mike Rosen, Charlotte Sellmyer
(202) 226-8417

Statement of Chairman Michael McCaul (R-Texas)
Committee on Homeland Security

"DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure"

March 13, 2013
Remarks as Prepared

I would like to thank all of our witnesses for testifying today. Deputy Secretary Lute is testifying for the Department but I look forward to seeing Secretary Napolitano in the coming weeks to discuss DHS' budget and its plan to maintain operations during these challenging times.

The chart on the screen depicts the roles of each major agency protecting our nation from cyber attacks.

The significance of this agreed-upon relationship to our national security is paramount. Each and every agency depicted understands their roles and responsibilities, working in tandem to keep America safe.

The purpose of this hearing is to examine the Department of Homeland Security's (DHS) role, capabilities and challenges concerning cybersecurity. There are many issues facing the Department.

Today's hearing is an opportunity to focus on the cyber threats facing our homeland and how together, we can defend against them.

Cyber attacks come in all forms. America is the victim of cyber espionage. Countries steal our military and intelligence information. There are threats of cyber-warfare from terrorists, and economic cyber attacks from Iran and China. These countries are stealing our trade secrets and intellectual property. The most daunting is undoubtedly the cyber threats against our critical infrastructure.

We know that foreign nations are conducting reconnaissance on our utilities – they are penetrating our gas and water systems and also our energy grids – and if the ability to send a silent attack through our digital networks falls into our enemies' hands, this country could be the victim of a devastating attack.

Yet while threats are imminent, no major cybersecurity legislation has been enacted since 2002.

Imagine months without power. An attack on our transformers could cripple our power grids and our economy would follow. This is not science fiction; it is reality. A report recently released by Mandiant confirmed China is the source of nearly 90% of cyber attacks against the United States. Most troubling is that these hackers targeted a company that provides remote access to more than 60% of North America's oil and gas pipelines.

Hackers have also attacked the servers of our Air Traffic Control System, and just last year, an al Qaeda operative issued a call for "electronic jihad" against the United States – comparing our technological vulnerabilities to that of our security before 9/11.

Iran and Russia are some of the world's worst offenders. Last December, Iranians attacked the state-owned Saudi Aramco, with the goal of stopping Saudi Arabia's oil production. Additionally, this year Iran conducted multiple denial of service attacks on major U.S. banks.

Unlike 9/11, we have seen the warning signs—now it is time to act. For us to defend against cyber attacks we must designate roles for all of the key agencies—DHS, DoD and the Justice Department. Each play a crucial role defending our homeland against cyber threats and none can do it alone.

When DHS was established, the Secretary of DHS was made responsible for "coordinating the overall national effort to enhance the protection of our critical infrastructure."

The National Infrastructure Protection Plan (NIPP) and the recent Executive Order solidified DHS' role as the lead federal agency in protecting domestic critical infrastructure.

Most importantly, the agencies themselves agree that a framework where DOJ is the lead for investigation, DHS is the lead for protection and DoD as the lead for defense would allow each

department to concentrate on their core mission with, as General Alexander once said, "…DHS as the entry point for working with industry."

In order to fulfill this role as a civilian command center, DHS has been building its partnerships with the private sector and growing its capacity as an effective conduit for threat information sharing. DHS manages a bottom-up network of entities from local first responders to nationwide threat analysis and emergency response centers like the National Cybersecurity and Communications Integration Center (NCCIC).

The Department possesses the ability to provide real time information necessary for instant threat detection, and to share emerging threat information to enable industry to act immediately to safeguard critical infrastructure. Additionally, DHS has a well-developed Privacy Office to protect Americans' privacy and civil liberties.

While the Department has made great progress, there are areas for further improvement across the board when dealing with cyber threats. Legal barriers, regulatory uncertainty and a lack of resources remain challenges. Additionally, there is not enough private sector participation in the programs that are already in place, because they either don't have the resources or don't see the value in doing so.

Congress has the ability and the obligation to help fix these problems. For us to thwart attacks, we must build upon the executive branch's efforts and work with all stakeholders to find the consensus necessary to protect this country. As part of this commitment, the Continuing Resolution recently passed by the House includes an increase of $282 million for cybersecurity over fiscal year 2012 levels.

Hearings like the one today will help guide the legislative process. I look forward to listening to all of our witnesses about what works, what doesn't and what we can do to streamline our cyber defenses.

One of the primary lessons from 9/11 is that only by working together can we detect and deter our enemies. In the wake of that tragedy, the walls preventing agencies from sharing threat information became apparent. We cannot allow turf battles to hinder us from developing the defenses necessary to prevent cyber attacks. The threat is real, and this time we see it coming.

###

Statement for the Record

"DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure"

Deputy Secretary Jane Hall Lute

U.S. Department of Homeland Security

Before the

House Committee on Homeland Security

March 13, 2013

Chairman McCaul, Ranking Member Thompson, and Members of the Committee:

I am pleased to join you today, and I thank the Committee for your strong support for the Department of Homeland Security (DHS) over the past four years and, indeed, since the Department's founding ten years ago.

I can think of no more urgent and important topic in today's interconnected world than cybersecurity, and I appreciate the opportunity to explain the Department's mission in this space and how we continue to improve cybersecurity for the American people as well as work to safeguard the nation's critical infrastructure and protect the Federal Government's networks.

Current Threat Landscape

Cyberspace is woven into the fabric of our daily lives. According to recent estimates, this global network of networks encompasses more than two billion people with at least 12 billion computers and devices, including global positioning systems, mobile phones, satellites, data routers, ordinary desktop computers, and industrial control computers that run power plants, water systems, and more.

While this increased connectivity has led to significant transformations and advances across our country – and around the world – it also has increased the importance and complexity of our shared risk. Our daily life, economic vitality, and national security depend on cyberspace. A vast array of interdependent IT networks, systems, services, and resources are critical to communication, travel, powering our homes, running our economy, and obtaining government services. No country, industry, community or individual is immune to cyber risks. The word "cybersecurity" itself encompasses protection against a broad range of malicious activity, from denial of service attacks, to theft of valuable trade secrets, to intrusions against government networks and systems that control our critical infrastructure.

The United States confronts a dangerous combination of known and unknown vulnerabilities in cyberspace and strong and rapidly expanding adversary capabilities. Cyber crime has also increased significantly over the last decade. Sensitive information is routinely stolen from both government and private sector networks, undermining the integrity of the data contained within these systems. We currently see malicious cyber activity from foreign nations engaged in espionage and information warfare, terrorists, organized crime, and insiders. Their methods range from distributed denial of service (DDoS) attacks and social engineering to viruses and other malware introduced through thumb drives, supply chain exploitation, and leveraging trusted insiders' access.

We have seen motivations for attacks vary from espionage by foreign intelligence services to criminals seeking financial gain and hackers who may seek bragging rights in the hacker community. Industrial control systems are also targeted by a variety of malicious actors who are usually intent on damaging equipment and facilities or stealing data. Foreign actors are also targeting intellectual property with the goal of stealing trade secrets or other sensitive corporate data from U.S. companies in order to gain an unfair competitive advantage in the global market.

Cyber attacks and intrusions can have very real consequences in the physical world. Last year, DHS identified a campaign of cyber intrusions targeting natural gas and pipeline companies that was highly targeted, tightly focused and well crafted. Stolen information could provide an attacker with sensitive knowledge about industrial control systems, including information that could allow for unauthorized operation of the systems. As the President has said, we know that our adversaries are seeking to sabotage our power grid, our financial institutions, and our air traffic control systems. These intrusions and attacks are coming all the time and they are coming from different sources and take different forms, all the while increasing in seriousness and sophistication.

The U.S. Government has worked closely with the private sector during the recent series of denial-of-service incidents. We have provided classified cyber threat briefings and technical assistance to help banks improve their defensive capabilities and we have increased sharing and coordination among the various government elements in this area. These developments reinforce the need for government, industry, and individuals to reduce the ability for malicious actors to establish and maintain capabilities to carry out such efforts.

In addition to these sophisticated attacks and intrusions, we also face a range of traditional crimes that are now perpetrated through cyber networks. These include child pornography and exploitation, as well as banking and financial fraud, all of which pose severe economic and human consequences. For example, in March 2012, the U.S. Secret Service (USSS) worked with U.S. Immigration and Customs Enforcement (ICE) to arrest nearly 20 individuals in its "Operation Open Market," which seeks to combat transnational organized crime, including the buying and selling of stolen personal and financial information through online forums. As Americans become more reliant on modern technology, we also become more vulnerable to cyber exploits such as corporate security breaches, social media fraud, and spear phishing, which targets employees through emails that appear to be from colleagues within their own organizations, allowing cyber criminals to steal information.

Cybersecurity is a shared responsibility, and each of us has a role to play. Emerging cyber threats require the engagement of our entire society—from government and law enforcement to the private sector and, most importantly, members of the public. The key question, then, is how do we address this problem? This is not an easy question because cybersecurity requires a layered approach. The success of our efforts to reduce cybersecurity risks depends on effective identification of cyber threats and vulnerabilities, analysis, and enhanced information sharing between departments and agencies from all levels of government, the private sector, international entities, and the American public.

Roles, Responsibilities, Activities

DHS is committed to ensuring cyberspace is supported by a secure and resilient infrastructure that enables open communication, innovation, and prosperity while protecting privacy, confidentiality, and civil rights and civil liberties by design.

Securing Federal Civilian Government Networks
DHS has operational responsibilities for securing unclassified federal civilian government networks and working with owners and operators of critical infrastructure to secure their networks through cyber threat analysis, risk assessment, mitigation, and incident response capabilities. We also are responsible for coordinating the national response to significant cyber incidents and for creating and maintaining a common operational picture for cyberspace across the government.

DHS directly supports federal civilian departments and agencies in developing capabilities that will improve their cybersecurity posture in accordance with the Federal Information Security Management Act (FISMA). To protect Federal civilian agency networks, our National Protection and Programs Directorate (NPPD) is deploying technology to detect and block intrusions through the National Cybersecurity Protection System and its EINSTEIN protective capabilities, while providing guidance on what agencies need to do to protect themselves and measuring implementation of those efforts.

NPPD is also developing a Continuous Monitoring as a Service capability, which will result in an array of sensors that feed data about an agency's cybersecurity risk and present those risks in an automated and continuously-updated dashboard visible to technical workers and managers to enhance agencies' ability to see and counteract day-to-day cyber threats. This capability will support compliance with Administration policy, be consistent with guidelines set forth by the National Institute of Standards and Technology (NIST), and enable Federal agencies to move from compliance-driven risk management to data-driven risk management. These activities will provide organizations with information necessary to support risk response decisions, security status information, and ongoing insight into effectiveness of security controls.

Protecting Critical Infrastructure
Critical infrastructure is the backbone of our country's national and economic security. It includes power plants, chemical facilities, communications networks, bridges, highways, and stadiums, as well as the federal buildings where millions of Americans work and visit each day. DHS coordinates the national protection, prevention, mitigation, and recovery from cyber incidents and works regularly with business owners and operators to take steps to strengthen their facilities and communities. The Department also conducts onsite risk assessments of critical infrastructure and shares risk and threat information with state, local and private sector partners.

Protecting critical infrastructure against growing and evolving cyber threats requires a layered approach. DHS actively collaborates with public and private sector partners every day to improve the security and resilience of critical infrastructure while responding to and mitigating the impacts of attempted disruptions to the nation's critical cyber and communications networks and to reduce adverse impacts on critical network systems.

DHS enhances situational awareness among stakeholders, including those at the state and local level, as well as industrial control system owners and operators, by providing critical cyber threat, vulnerability, and mitigation data, including through Information Sharing and Analysis Centers, which are cybersecurity resources for critical infrastructure sectors. DHS is also home to the National Cybersecurity & Communications Integration Center (NCCIC), a 24x7 cyber

situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

Responding to Cyber Threats

DHS is responsible for coordinating the Federal Government response to significant cyber or physical incidents affecting critical infrastructure. Since 2009, the NCCIC has responded to nearly half a million incident reports and released more than 26,000 actionable cybersecurity alerts to our public and private sector partners. The DHS Office of Intelligence and Analysis is a key partner in NCCIC activities, providing tailored all-source cyber threat intelligence and warning to NCCIC components and public and private critical infrastructure stakeholders to prioritize risk analysis and mitigation.

An integral player within the NCCIC, the U.S. Computer Emergency Readiness Team (US-CERT) also provides response support and defense against cyber attacks for Federal civilian agency networks as well as private sector partners upon request. US-CERT collaborates and shares information with state and local government, industry, and international partners, consistent with rigorous privacy, confidentiality, and civil liberties guidelines, to address cyber threats and develop effective security responses. In 2012, US-CERT processed approximately 190,000 cyber incidents involving Federal agencies, critical infrastructure, and our industry partners. This represents a 68 percent increase from 2011. In addition, US-CERT issued over 7,455 actionable cyber-alerts in 2012 that were used by private sector and government agencies to protect their systems, and had over 6,400 partners subscribe to the US-CERT portal to engage in information sharing and receive cyber threat warning information.

The Department's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) also responded to 177 incidents last year while completing 89 site assistance visits and deploying 15 teams with US-CERT to respond to significant private sector cyber incidents. DHS also empowers owners and operators through a cyber self-evaluation tool, which was used by over 1,000 companies last year, as well as in-person and on-line training sessions.

Successful response to dynamic cyber threats requires leveraging homeland security, law enforcement, and military authorities and capabilities, which respectively promote domestic preparedness, criminal deterrence and investigation, and national defense. DHS, the Department of Justice (DOJ), and the Department of Defense (DOD) each play a key role in responding to cybersecurity incidents that pose a risk to the United States. In addition to the aforementioned responsibilities of our Department, DOJ is the lead Federal department responsible for the investigation, attribution, disruption, and prosecution of domestic cybersecurity incidents while DOD is responsible for securing national security and military systems as well as gathering foreign cyber threat information and defending the nation from attacks in cyberspace. DHS supports our partners in many ways. For example, the United States Coast Guard as an Armed Force has partnered with U.S. Cyber Command and U.S. Strategic Command to conduct military cyberspace operations.

While each agency operates within the parameters of its authorities, the U.S. Government's response to cyber incidents of consequence is coordinated among these three agencies such that "a call to one is a call to all." Synchronization among DHS, DOJ, and DOD not only ensures

that whole of government capabilities are brought to bear against cyber threats, but also improves government's ability to share timely and actionable cybersecurity information among a variety of partners, including the private sector.

Combating Cybercrime

DHS employs more law enforcement agents than any other Department in the Federal Government and has personnel stationed in every state and in more than 75 countries around the world. To combat cyber crime, DHS relies upon the skills and resources of the USSS and ICE and works in cooperation with partner organizations to investigate cyber criminals. Since 2009, DHS has prevented $10 billion in potential losses through cyber crime investigations and arrested more than 5,000 individuals for their participation in cyber crime activities.

The Department leverages the 31 USSS Electronic Crimes Task Forces (ECTF), which combine the resources of academia, the private sector, and local, state and Federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructure. A recently executed partnership between ICE Homeland Security Investigations and USSS demonstrates the Department's commitment to leveraging capability and finding efficiencies. Both organizations will expand participation in the existing ECTFs. In addition to strengthening each agency's cyber investigative capabilities, this partnership will produce benefits with respect to the procurement of computer forensic hardware, software licensing, and training that each agency requires. The Department is also a partner in the National Cyber Investigative Joint Task Force, which serves as a collaborative entity that fosters information sharing across the interagency.

We work with a variety of international partners to combat cybercrime. For example, through the U.S.-EU Working Group on Cybersecurity and Cybercrime, which was established in 2010, we develop collaborative approaches to a wide range of cybersecurity and cybercrime issues. In 2011, DHS participated in the Cyber Atlantic tabletop exercise, a U.S.–EU effort to enhance international collaboration of incident management and response, and in 2012, DHS and the EU signed a joint statement that advances transatlantic efforts to enhance online safety for children. ICE also works with international partners to seize and destroy counterfeit goods and disrupt websites that sell these goods. Since 2010, ICE and its partners have seized over 2,000 domain names associated with businesses selling counterfeit goods over the Internet. To further these efforts, the Administration issued its Strategy on Mitigating the Theft of U.S. Trade Secrets last month. DHS will act vigorously to support the Strategy's efforts to combat the theft of U.S. trade secrets – especially in cases where trade secrets are targeted through illicit cyber activity by criminal hackers.

In addition, the National Computer Forensic Institute has trained more than 1,000 state and local law enforcement officers since 2009 to conduct network intrusion and electronic crimes investigations and forensic functions. Several hundred prosecutors and judges as well as representatives from the private sector have also received training on the impact of network intrusion incident response, electronic crimes investigations, and computer forensics examinations.

Building Partnerships
DHS serves as the focal point for the Government's cybersecurity outreach and awareness efforts. Raising the cyber education and awareness of the general public creates a more secure environment in which the private or financial information of individuals is better protected. For example, the Multi-State Information Sharing and Analysis Center (MS-ISAC) opened its Cyber Security Operations Center in November 2010, which has enhanced NCCIC situational awareness at the state and local government level and allows the Federal Government to quickly and efficiently provide critical cyber threat, risk, vulnerability, and mitigation data to state and local governments. MS-ISAC has since grown to include all 50 states, three U.S. territories, the District of Columbia, and more than 200 local governments.

The Department also has established close working relationships with industry through partnerships like the Protected Critical Infrastructure Information (PCII) Program, which enhances voluntary information sharing between infrastructure owners and operators and the government. The Cyber Information Sharing and Collaboration Program established a systematic approach to cyber threat information sharing and collaboration between critical infrastructure owners and operators across the various sectors. And, in 2010, we launched a national campaign called *Stop.Think.Connect* to spread public awareness about how to keep our cyber networks safe.

In addition, DHS works closely with international partners to enhance information sharing, increase situational awareness, improve incident response capabilities, and coordinate strategic policy issues in support of the Administration's International Strategy for Cyberspace. For example, the Department has fostered international partnerships in support of capacity building for cybersecurity through agreements with Computer Emergency Response and Readiness Teams as well as the DHS Science & Technology Directorate (S&T). Since 2009, DHS has established partnerships with Australia, Canada, Egypt, India, Israel, the Netherlands, and Sweden.

Fostering Innovation
The Federal Government relies on a variety of stakeholders to pursue effective research and development projects that address increasingly sophisticated cyber threats. This includes research and development activities by the academic and scientific communities to develop capabilities that protect citizens by enhancing the resilience, security, integrity, and accessibility of information systems used by the private sector and other critical infrastructure. DHS supports Centers of Academic Excellence around the country to cultivate a growing number of professionals with expertise in various disciplines, including cybersecurity.

DHS S&T is leading efforts to develop and deploy more secure internet protocols that protect consumers and industry internet users. We continue to support leap-ahead research and development, targeting revolutionary techniques and capabilities that can be deployed over the next decade with the potential to redefine the state of cybersecurity in response to the Comprehensive National Cybersecurity Initiative. For example, DHS was a leader in the development of protocols at the Internet Engineering Task Force called Domain Name System Security (DNS SEC) Extensions. DNS SEC is necessary to protect internet users from being covertly redirected to malicious websites and helps prevent theft, fraud, and abuse online by

blocking bogus page elements and flagging pages whose Domain Name System (DNS) identity has been hijacked. S&T is also driving improvements through a Transition to Practice Program as well as liability and risk management protections provided by the Support Anti-Terrorism by Fostering Effective Technology (SAFETY) Act that promote cyber security technologies and encourage their transition into successful use.

Growing and Strengthening our Cyber Workforce
We know it only takes a single infected computer to potentially infect thousands and perhaps millions of others. But at the end of the day, cybersecurity is ultimately about people. The most impressive and sophisticated technology is worthless if it's not operated and maintained by informed and conscientious users.

To help us achieve our mission, we have created a number of competitive scholarship, fellowship, and internship programs to attract top talent. We are growing our world-class cybersecurity workforce by creating and implementing standards of performance, building and leveraging a cybersecurity talent pipeline with secondary and post-secondary institutions nationwide, and institutionalizing an effective, ongoing capability for strategic management of the Department's cybersecurity workforce. Congress can support this effort by pursuing legislation that provides DHS with the hiring and pay flexibilities we need to secure Federal civilian networks, protect critical infrastructure, respond to cyber threats, and combat cybercrime.

Recent Executive Actions

As discussed above, America's national security and economic prosperity are increasingly dependent upon the cybersecurity of critical infrastructure. With today's physical and cyber infrastructure growing more inextricably linked, critical infrastructure and emergency response functions are inseparable from the information technology systems that support them. The government's role in this effort is to share information and encourage enhanced security and resilience, while identifying and addressing gaps not filled by the market-place.

Last month, President Obama issued Executive Order 13636 on Improving Critical Infrastructure Cybersecurity as well as Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience, which will strengthen the security and resilience of critical infrastructure through an updated and overarching national framework that acknowledges the increased role of cybersecurity in securing physical assets.

DHS Responsibilities
The President's actions mark an important milestone in the Department's ongoing efforts to coordinate the national response to significant cyber incidents while enhancing the efficiency and effectiveness of our work to strengthen the security and resilience of critical infrastructure. The Executive Order supports more efficient sharing of cyber threat information with the private sector and directs NIST to develop a Cybersecurity Framework to identify and implement better security practices among critical infrastructure sectors. The Executive Order directs DHS to establish a voluntary program to promote the adoption of the Cybersecurity Framework in conjunction with Sector-Specific Agencies and to work with industry to assist companies in implementing the framework.

The Executive Order also expands the voluntary DHS Enhanced Cybersecurity Service program, which promotes cyber threat information sharing between government and the private sector. This engagement helps critical infrastructure entities protect themselves against cyber threats to the systems upon which so many Americans rely. This program is a good example of information sharing with confidentiality, privacy and civil liberties protections built into its structure. DHS will share with appropriately cleared private sector cybersecurity providers the same threat indicators that we rely on to protect the .gov domain. Those providers will then be free to contract with critical infrastructure entities and provide cybersecurity services comparable to those provided to the U.S. Government.

Through the Executive Order, the President also directed agencies to incorporate privacy, confidentiality, and civil liberties protections. It specifically instructs DHS to issue a public report on activities related to implementation, which would therefore enhance the existing privacy policy, compliance, and oversight programs of DHS and the other agencies.

In addition, the Presidential Policy Directive directs the executive branch to strengthen our capability to understand and efficiently share information about how well critical infrastructure systems are functioning and the consequences of potential failures. It also calls for a comprehensive research and development plan for critical infrastructure to guide the government's effort to enhance market-based innovation.

Because the vast majority of U.S. critical infrastructure is owned and operated by private companies, reducing the risk to these vital systems requires a strong partnership between government and industry. There is also a role for state, local, tribal and territorial governments who own a significant portion of the nation's critical infrastructure. In developing these documents, the Administration sought input from stakeholders of all viewpoints in industry, government, and the advocacy community.

Their input has been vital in crafting an order that incorporates the best ideas and lessons learned from public and private sector efforts while ensuring that our information sharing incorporates rigorous protections for individual privacy, confidentiality, and civil liberties. Indeed, as we perform all of our cyber-related work, we are mindful of the need to protect privacy, confidentiality, and civil liberties. The Department has implemented strong privacy and civil rights and civil liberties standards into all its cybersecurity programs and initiatives from the outset. To accomplish the integrated implementation of these two directives, DHS has

established an Interagency Task Force made up of representatives from across all levels of government.

Continuing Need for Legislation

It is important to note that the Executive Order directs Federal agencies to work within current authorities and increase voluntary cooperation with the private sector to provide better protection for computer systems critical to our national and economic security. It does not grant new regulatory authority or establish additional incentives for participation in a voluntary program. We continue to believe that a suite of legislation is necessary to implement the full range of steps needed to build a strong public-private partnership, and we will continue to work with Congress to achieve this.

The Administration's legislative priorities for the 113th Congress build upon the President's 2011 Cybersecurity Legislative Proposal and take into account two years of public and congressional discourse about how best to improve the nation's cybersecurity. Congress should enact legislation to incorporate privacy, confidentiality, and civil liberties safeguards into all aspects of cybersecurity; strengthen our critical infrastructure's cybersecurity by further increasing information sharing and promoting the establishment and adoption of standards for critical infrastructure; give law enforcement additional tools to fight crime in the digital age; and create a National Data Breach Reporting requirement.

Conclusion

The American people expect us to secure the country from the growing danger of cyber threats and ensure the nation's critical infrastructure is protected. The threats to our cybersecurity are real, they are serious, and they are urgent.

I look forward to working with this Committee and the Congress to ensure we continue to take every step necessary to protect cyberspace, in partnership with government at all levels, the private sector, and the American people, and continue to build greater resiliency into critical cyber networks and systems.

I appreciate this Committee's guidance and support as together we work to keep our nation safe. Thank you, again, for the attention you are giving to this urgent matter.

Testimony of

Mr. Anish Bhimani

On behalf of the

Financial Services Information Sharing and Analysis Center (FS-ISAC)

before the

Committee on Homeland Security

United States House of Representatives

"DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure"

March 6, 2013

STATEMENT FOR THE RECORD

Chairman McCaul, Ranking Member Thompson, and members of the Committee, my name is Anish Bhimani, and I am the Chief Information Risk Officer of JPMorgan Chase & Co. I am appearing today as the Chair of the Financial Services Information Sharing and Analysis Center (FS-ISAC). I thank you for the opportunity to address the Committee on the important topic of roles and responsibilities of the government and private sector in the critical area of cybersecurity.

I would like to address a few points today: first, an overview of the FS-ISAC, its charter, purpose and membership; lessons learned with regard to information sharing; perspectives on the FS-ISAC membership's interaction with government agencies; and finally, recommendations around information sharing and cybersecurity governance.

FS-ISAC Background

The FS-ISAC was established in 1999 in response to Presidential Decision Directive 63. This directive, later updated by Homeland Security Presidential Directive 7, required public and private sector organizations to share information about cyber threats and vulnerabilities, with the goal of helping protect the nation's critical infrastructure. The FS-ISAC is a nonprofit organization funded entirely by its member firms and sponsors. Its membership is comprised of thousands of financial and banking institutions, large and small, and its mission is straightforward – to provide the primary industry forum for collaboration on the critical cybersecurity threats facing the financial services sector. From 12 founding members at its inception, the FS-ISAC has grown to over 4,400 organizations, including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, exchanges and clearing houses,

payments processors, and over 30 trade associations, representing the majority of the U.S. financial services sector.

The overall objective of the FS-ISAC is to provide the financial services sector with the information it needs to defend against cyber threats and risk. It acts as a trusted third party that allows members to share threat, vulnerability and incident information in a timely, trusted, and, if desired, anonymous manner. FS-ISAC information sharing services and activities include:

- Delivery of timely, relevant and actionable alerts from various sources distributed through the FS-ISAC Security Operations Center (SOC);
- Trusted mechanisms to facilitate member sharing of threat, vulnerability and incident information, in either an attributed or non-attributed manner;
- Sector-specific groups and subcommittees that provide forums for members in a given part of the sector, e.g., the Payment Processors Information Sharing Council (PPISC), Insurance Risk Council, Payments Risk Council, Community Institutions Council, and the Clearing House and Exchange Forum (CHEF);
- Bi-weekly threat information sharing calls for members and invited security/risk experts to discuss the latest threats, vulnerabilities and incidents affecting the sector;
- Engagement with private security companies to identify threat information of relevance to the membership and the sector;
- Development of risk mitigation best practices, threat viewpoints and toolkits, as well as member-driven research regarding best practices at member organizations;
- Subject Matter Expert committees, including the Threat Intelligence and Business Resilience Committees, which provide in-depth analysis of risks to the sector, and provide technical, business and operational impact assessments, as well as strategies to mitigate risk; and
- Participation in sector, cross-sector and national exercises and drills, such as the Cyber Attacks Against Payment Processes (CAPP), National Level Exercise 2012, and the Cyber Storm series.

Despite the competitive nature of our industry, members of the FS-ISAC recognize that the threat from cyber attacks affects all of us, and that defending the nation's critical infrastructure is not a competitive issue. We all recognize that to effectively combat this threat, we must come together as a sector and leverage the full capabilities of our collective membership. We also know that we must trust one another. Trust, simply put, is the key to the success of the FS-ISAC, and any information sharing model.

Trust is not something that can be mandated, nor easily earned. Indeed, over the past 14 years, FS-ISAC members have worked tirelessly to engender trust amongst each other and are using all of the capabilities listed above to promote the flow of threat information across the sector. As an example, the FS-ISAC has built a model for sharing information in an authenticated, but anonymous, manner for those organizations that wish to take advantage of it. In addition, we have instituted a "traffic light" protocol, indicating levels of information sensitivity and how

information may be disseminated to the membership, partners, and other organizations. These mechanisms have effectively and efficiently enabled the amount of information shared among FS-ISAC members to grow from a mere trickle a few years ago, to a veritable (but manageable) flood today. In January 2013, members shared over 92,000 pieces of threat intelligence and approximately 400 events across the sector.

U.S. Government Interaction

Equally critical as industry collaboration is our partnership with government agencies. We could not protect ourselves against cyber attacks without extremely close collaboration, partnership, and most importantly, information sharing, with a number of government agencies – most notably, the U.S. Department of Treasury and the Department of Homeland Security, but also the Federal Reserve, Office of the Comptroller of the Currency, United States Secret Service, U.S. Cyber Command, Federal Bureau of Investigation, National Security Agency, Central Intelligence Agency, and state and local governments. Additionally, the FS-ISAC is a member of, and partner to, the Financial Services Sector Coordinating Council (FSSCC) for Homeland Security and Critical Infrastructure Protection, established under HSPD7, and works extremely closely with the Financial and Banking Information Infrastructure Committee (FBIIC), under the auspices of the President's Working Group on Financial Markets. These organizations and relationships are part of the financial sector's long history of public-private partnership with various government agencies in the area of cybersecurity.

One example of this partnership is the successful effort by the Department of Treasury, Homeland Security, FBI, U.S. Secret Service and other partners to obtain over 250 secret-level clearances and several TS/SCI clearances for key financial services sector personnel. These clearances have enabled FS-ISAC members to receive briefings on new security threats and have provided useful information to the sector to implement effective controls and defenses to combat these threats. We know that this process is not always easy, and that sponsoring private sector clearances has, historically, been difficult. But in our view, given how much cyber information is classified, it is absolutely essential that private sector representatives have access to this information. The FS-ISAC would like to see this process updated and expanded to provide more clearances to the private sector, and make it easier for this information to be shared more broadly and quickly with our members.

Another good example of partnership is the work of the National Cybersecurity & Communications Integration Center (NCCIC) at DHS. In June 2011, the FS-ISAC became the fourth private sector organization to place staff on the floor at the NCCIC. Specifically, FS-ISAC representatives, cleared at the Top Secret/SCI level, attend NCCIC daily briefs and other meetings to share information on threats, vulnerabilities, incidents, and potential impacts to the sector. These individuals interact on a daily basis with the NCCIC, routinely submit and respond to requests for information, collaborate on analyses and work with the NCCIC staff to determine what information from the NCCIC would be of use to our members, and what can be shared with whom. Over the past 18 months in particular, our presence on the NCCIC floor has greatly enhanced situational awareness and information sharing between the sector and the government, as well as across other critical infrastructure sectors that participate on the floor.

More recently, the FS-ISAC has embedded a full-time staff person on the NCCIC floor in addition to the part-time resources that were deployed last year.

One of the high points in the public-private partnership with the sector occurred in 2011 when a pilot program, known as the Government Information Sharing Framework (GISF) was launched with the Defense Department. Under the program, an initial 16 financial services firms (with a plan to expand participation later) were granted access to advanced threat information, as well as to classified analysis on threat actors and mitigation techniques. The GISF provided an invaluable service to the sector, enabling the pilot participants to receive actionable, timely, and contextual information that allowed them to search for similar threat activity in their own environments. It also allowed private sector participants to adjust their assessments of cyber espionage threats using intelligence that had previously been unavailable. The program jumpstarted new efforts across the industry and helped reshape the sector's approach to assessing cyber espionage risks.

Unfortunately, the Department of Defense terminated the pilot program in December 2011 due to funding limitations. The GISF was a significant leap forward in the public-private partnership, and represented a critical line of defense in mitigating the growing cyber threat. The loss of that information feed has already been felt, as numerous financial institutions have experienced activity from actors first identified through GISF reporting and intelligence. The FS-ISAC strongly supports not only restarting the GISF program, but also expanding its reach across the financial services sector. We urge Congress and the Department of Defense to resolve any outstanding funding or authorization issues and reinstate this crucial program.

As you can see, the financial services sector, and the FS-ISAC in particular, work in collaboration with a wide range of government agencies – probably more than anyone would imagine. At the same time, we benefit from having a strong sector-specific agency – the Treasury Department – that allows us to navigate the various government agencies involved in cybersecurity.

Specifically, the Treasury's Office of Critical Infrastructure Protection plays an invaluable role to the sector, serving as a conduit between our members and the various government agencies that play a role in critical infrastructure protection. We believe that, given its knowledge of the financial services industry, as well as its relationship with various intelligence agencies, Treasury is uniquely qualified to serve in that role. Regardless of which organization is involved, however, the key is that we receive timely, actionable data from the appropriate source, whoever that is, so that we can take the appropriate action.

Creating a useful information sharing framework

There are two critical elements to creating a useful information sharing framework: determining what information should be shared, and developing robust processes for sharing timely information.

In thinking through this problem, it is impossible to construct an effective information sharing framework without also considering what specific information we need to share to most effectively protect our infrastructure. Although much of the current debate around information

sharing has focused on the important goal of protecting personal information, we believe that much could be accomplished without ever sharing personally identifiable information.
With that in mind, here are a few examples of information we at FS-ISAC believe would be most helpful to share:

- Technical details of cyber attacks as seen on networks, in IT systems, or by victims, including IP addresses of attackers and their networks;
- Analytic content of incidents, attack patterns, and trends without revealing the organization affected;
- Analysis of technical details to determine the techniques, tools, and procedures that adversaries are using to target victim organizations;
- Contextual information about threat actor groups and campaigns;
- Information about the motivation, objectives, and capabilities of these groups or campaigns.

In addition to those most critical data elements we think must be shared, we also believe that critical infrastructure owners and operators would benefit from having a much stronger framework around *how* we share.

The cybersecurity threats the financial industry faces are coming at us faster than ever before, and are growing increasingly complex. As a result, receiving stale and outdated information is of very little value in protecting our infrastructure – in fact, it is a drain on resources, and a waste of valuable time. We are strong advocates of a framework where our respective agencies and companies can deliver relevant information very quickly, at network speed, with that information flowing in both directions.

Why is that important? Today, we in the private sector face attacks that were once directed only against major government institutions. Government agencies may have established strategies and tactics to deal with those attacks that would be valuable to those us facing similar threats. Likewise, the financial sector has collectively established strategies and tactics that may be of use to government agencies. Sharing these strategies and tools to deal with advanced threats comprehensively and quickly would do a great deal to help us all fight advanced attackers.

Conclusion

In closing, please accept my thanks on behalf of the FS-ISAC for the opportunity to address the Committee on this critical issue. The risks associated with cyber attacks and threats are real, and of paramount importance to the financial industry as a whole. The ability to share information across the sector, as well as with our partners in government and law enforcement, while still protecting privacy and civil liberties, is core to our industry and our nation's response to the growing threat.

I look forward to any questions the Committee may have.

Gary W. Hayes

Division Vice President & Chief Information Officer

CenterPoint Energy, Inc.

****

Testimony before the House Committee on Homeland Security

****

"DHS Cyber Security: Roles and Responsibilities to Protect the Nation's Critical Infrastructure"

March 6, 2013

Overview

Chairman McCaul, Ranking Member Thompson, and Members of the Committee, my name is Gary Hayes and I am the Chief Information Officer for CenterPoint Energy. Thank you for inviting me to testify on my experiences and perspectives on protecting critical infrastructure from cyber attacks.

CenterPoint Energy, Inc. ("CenterPoint Energy"), headquartered in Houston, Texas, is a domestic energy delivery company that includes electric transmission and distribution, natural gas local distribution, natural gas gathering and processing, interstate pipelines and competitive natural gas sales and services. It has assets totaling more than $21 billion. Our company has approximately 8,800 employees and serves more than 5 million metered customers primarily in Arkansas, Louisiana, Minnesota, Mississippi, Oklahoma and Texas.

As the CIO of CenterPoint Energy I am accountable for our cyber security programs and have direct responsibility for our corporate business systems' cyber security. Because of the diverse segments of the energy infrastructure in which CenterPoint Energy's companies participate, I coordinate, collaborate, and communicate with our operational technology functions to define policies, procedures, practices and programs in our efforts to provide cyber security. I have a highly dedicated, educated and capable team executing responsibilities in this effort.

I also have the responsibility to represent and coordinate representation of our company in industry and government efforts focused on cyber security.

We focus heavily on participation in relevant industry groups. I participate on the American Gas Association ("AGA") and Edison Electric Institute ("EEI") Cyber Task Groups and I coordinate with David Jewell, Senior Vice President, Commercial Operations, Optimization and Gas System, who represents CenterPoint Energy on the Cyber Task Group for the Interstate Natural Gas Association of America ("INGAA"). We also participate in numerous governmental, private and industry-related efforts focused on cyber security.

Our cyber security technologies operate across three areas: interstate pipelines, local gas distribution utilities and an electric utility. For cyber security purposes, our interstate natural gas transmission pipelines are under the jurisdiction of the Transportation Security Administration ("TSA"). Our local gas distribution companies operate under the same jurisdiction but, for cyber security purposes, have no single regulator because some of the Federal authority has been delegated to the states. And, finally, CenterPoint Energy's electric utility in the Houston, operates under the jurisdiction of the Federal Energy Regulatory Commission ("FERC") for compliance with North American Electric Corporation reliability standards. We also work voluntarily with a multitude of other groups including the Federal Bureau of Investigation, Industrial Controls Systems Cyber Emergency Response Team (ICS-CERT) and the Department of Energy (DOE) and, of course, Department of Homeland Security (DHS).

My goal today is to share CenterPoint Energy's perspective with regards to cyber security challenges, activities and opportunities. That perspective is this: cyber threats are evolving and require collaboration, information sharing with the government and continued collaboration with the industry to effectively protect the nation's critical infrastructure. Our goal is to focus our resources on facing the cyber threat.

This perspective is shaped by our experiences and participation in industry groups as well as our collaboration with several governmental agencies including the DOE, DHS and the TSA. Furthermore, our relationship with members of our supply chain, our suppliers and vendors, is critical. From these experiences, we have determined that we need the ability to respond in a quick and agile manner, as well as continuously improve our capabilities to respond. Collaboration is the key.

As a critical energy transporter and distributor to the nation, we know that we have responsibilities to the public, our customers and our shareholders. We have prioritized our cyber security efforts in parallel with our corporate philosophy.

1. Public Safety

2. Energy Delivery

3. Customer Service

I hope this document provides a helpful "participant's view and perspective" as we work together to protect our Company and our nation's critical infrastructure.

Cyber Security Efforts and Collaboration

CenterPoint Energy has a long history of safe and reliable energy delivery to our customers. Our team members take pride in getting up every morning with this mission top of mind. To this point, we take protection of the public, our control systems, customer and employee information, critical infrastructure information, and intellectual property very seriously. Cyber security has been incorporated into our processes, procedures, and operations through various mechanisms over time. But, we do recognize that the current cyber environment has escalated beyond historical expectations and our efforts must and will continue to evolve in order to meet these dynamic and ever-evolving threats.

We have evolved from a strategy of "perimeter defense" (e.g., keep the bad actors out) to a strategy of "depth-in-defense" (recognition that technology system perimeters were susceptible to compromise, depth-in-defense provides increased reliance on detection and response mechanisms to address threats within the protection perimeter). We have established objectives, techniques, talent and tools to assist us in our current efforts. We have also focused on educating our workforce, as they represent the first line of defense. However, we recognize our cyber security capabilities must continue to evolve. This recognition comes from education and collaboration with industry and government. Our objectives are to mature and enhance our strategy and move to an "agile defense".[1] In particular, we will enhance our focus on the people, processes and technologies that can be managed, monitored, tested, measured and continuously improved.

As an important part of the energy delivery value chain, we are also enhancing resiliency, which is our ability to respond quickly to attacks and to maintain critical services. As we have learned through our participation in many of the cyber discussions, "bad actors will get in". It is not a matter of "if" but a matter of "when." Therefore, we continue to evolve our capability to respond and operate in a compromised state.

Identifying and coordinating with the right stakeholders is vital to that evolution.

[1] An enhanced comprehensive security strategy referred to by NIST as "agile defense". Agile defense combines traditional perimeter, depth-in-defense and depth-in-breadth, which is a planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the life cycle. Life cycle is the network that includes product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement.

First, we believe that participation with industry coalitions is critical. Our collaboration with fellow energy sector members allows us to continually learn and incorporate leading practices, provide mutual assistance and educate stakeholders and policy makers of real risks and possible solutions. We encourage and assist in collaboration between AGA, EEI, INGAA and key policymakers.

Second, collaboration between the public and private sector is a vital part of cyber protection. Deployment of the SmartGrid in Houston presented us with the opportunity to work with DOE, DHS and other federal agencies in order to successfully deliver advanced metering capabilities. Throughout the process, we collaborated with government stakeholders to incorporate customer protection and cyber security into our design and operations. This could not have been achieved without information sharing, a focus on quality and integrity, strong risk management, and joint objectives - all of these achieved through collaboration.

Those partnerships are also critical for our intelligent grid project and we look forward to continuing those relationships.

Other examples illustrating the success of public-private partnerships are the joint industry and governmental initiatives that developed the electric sector cyber security Capability Maturity Model, guidelines for the natural gas pipeline sectors' Pipeline Security Guidelines and many more activities that have benefited CenterPoint Energy and our industry. These collaborative efforts focused on targeted objectives and provided tangible programs, information, tools, techniques, and knowledge to help us enhance our efforts in this war against cyber threats. We encourage Congress to promote continued focus on private and public partnerships for the protection of our national security.

And, finally, cyber security collaboration must take into account the entire life cycle and supply chain. Therefore, we must recognize the essential participation of our vendors and suppliers in this effort. They have worked with us to provide products and solutions to meet the demands of this challenge. Our joint goals and efforts focus on design, testing, and improvement of products to understand quality, integrity, risks, threats, mitigations and management of these solutions in our operating environment.

Cyber Security Participant Observations

There is a set of common themes that we see emerging from our cyber security efforts and dialogues:

Shared Goals: Identifying and merging the focus and priorities of the stakeholders is a key to success.

Risk Based Approach: A risk based approach is fundamental to our efforts. Goals should be prioritized and articulated clearly. Solutions should be focused and yet flexible. A "one size fits all" approach won't work for unique problems. There are utility service providers serving hundreds of customers and others serving millions of customers; therefore, the risk profile will influence the objectives, techniques and tools to effectively manage cyber security.

Information Sharing and Situational Awareness: We desire a defined collaborative process to share information in a quick, secure and non-prejudicial fashion. That process should educate us in ways that we can be proactive and not reactive. Throughout many conferences, meetings, calls and other interactions, we continue to hear that the ICS-CERT serves as a strong template for developing a working model of collaboration. "Boots on the ground" security team members find this of great value in their efforts in the cyber war. We believe this is an example of information sharing that provides actionable information, support to our industry, and brings value to public-private partnership.

Leveraging Tools and Techniques: Although we, and many others, employ market-leading technologies and information solutions, we believe our effort would be greatly enhanced by leveraging cyber technologies and solutions utilized by governmental organizations and fellow industry members. We recognize there are many obstacles, but today's cyber security challenges require us to remove these obstacles and provide a repeatable and supportable path to facilitate results. Each day of delay is another day of opportunity for advanced persistent threat actors.

Security Clearance: Expanded security and expedited clearance for appropriate personnel within the private sector and expedited communication of critical information is critical to the ability of owners and operators to be proactive and responsive to emerging threats. We were pleased to see such a provision in the President's Executive Order on cyber security.

Cyber Security Regime: A cyber security framework must prioritize the principle that agility is the key to responding to cyber threats. An overly burdensome and prescriptive regulatory regime will be increasingly challenged to keep pace with evolving cyber threats. A beneficial framework not only defines capabilities, but provides learning, methodologies, objectives and techniques (tools and measures) to achieve the required results. In conjunction with risk-based analysis, that type of framework can be leveraged by all participants to mitigate threats.

Incident Management: The reality is advanced persistent threat actors are not going away and the risk of a cyber incident will remain top of mind for the foreseeable future. Increased situational awareness coupled with response and recovery plans will be incorporated into existing emergency operating procedures.

A leading effort on incident management comes under the auspices of the National Infrastructure Advisory Council (NIAC) report, several electric utility CEOs are engaged in an ongoing partnership with the White House National Security Staff and senior officials throughout the government, including Department of Energy Deputy Secretary Daniel Poneman and Department of Homeland Security Deputy Secretary Jane Holl Lute. This collaboration has resulted in several government-industry initiatives, one of which is to identify roles and responsibilities that will expedite response and recovery should a major power disruption occur.

Collaboration: All of these themes require partnerships with industry and government. Collaboration is essential to our combined mission of protecting the public, customers, employees, critical infrastructure, intellectual property and national security. Notable examples demonstrating the strength of collaboration between public and private sectors include the Industrial Control Systems Joint Work Group (ICS-JWG) and the TSA-sponsored public-private partnership which supports the National Infrastructure Protection Plan (NIPP).

To illustrate further, I offer the case of our interstate gas transmission pipelines where the cyber collaboration with the federal government began through our work with INGAA and AGA. After the September 11 attacks, and before the TSA or the DHS were created, we voluntarily collaborated through INGAA and AGA with the then Research and Special Programs Administration within the Department of Transportation (DOT) to develop the initial Pipeline Security Information Circular. This collaborative approach to developing and implementing security measures continues to this day in our collaboration with the TSA. Since that time, gas pipeline owners and operators have worked with TSA to safeguard and protect our infrastructure's security – both from physical and cyber attacks. As a result of years of work and collaboration between owners and operators and the TSA we have a strong, trust-based collaboration – a public-private partnership. This approach, and the relationship it fostered, produced robust, thorough cyber guideline development for natural gas transmission pipelines even before the "911 Act" became law.[2]

TSA is using a voluntary partnership approach because it works. TSA and the private sector partner in order to leverage the collective expertise and experience of the government and private industry in finding practical solutions to cyber security. This approach and the relationship it has fostered have produced robust cyber security guidelines and best practices for natural gas transmission pipelines.

The TSA approach builds on what has been proven through experience: public-private partnerships for cyber security generate solutions. A Congressional Research Service August 2012 report, "Pipeline Cyber Security: Federal Policy," stated that "TSA officials assert that

[2] Implementing Recommendations of the 9/11 Commission Act.

security regulations could be counter-productive because they could establish a general standard below the level of security already in place at many pipeline companies based on their company-specific security assessments." Moreover, the report notes that "[b]ecause TSA believes the most critical U.S. pipeline systems generally meet or exceed industry security guidance, the agency believes it achieves better security with voluntary guidelines, and maintains a more cooperative and collaborative relationship with its industry partners as well."

We believe that the key to effective cyber security is the trust developed in partnerships like the one with TSA. The dynamic solutions that are born of the public and private sector coming together are not possible when the government is only acting as a regulator and enforcer. The cyber security world moves too quickly for such traditional regulatory models to be beneficial or productive.

Conclusion

We take seriously the responsibility of protecting our customers, employees, assets, and communities in which we operate, and thus cyber security is a top priority for CenterPoint Energy. We also recognize the importance of critical infrastructure to our national security. Because cyber threats are constantly changing and evolving, we support voluntary programs that encourage partnership, collaboration, sharing of information and technology, and the preparedness necessary to mitigate and respond to the ever changing nature of cyber attacks. We will not succeed in this effort alone. The strengthening and expansion of industry and government partnerships provides our best front in this cyber war.

Chairman McCaul, Ranking Member Thompson, and Members of the Committee, we appreciate the opportunity to share our perspectives and stand ready to assist you in your efforts to protect our critical infrastructure.

Written Statement of

Michelle Richardson, Legislative Counsel

American Civil Liberties Union

Washington Legislative Office

On

"DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure"

Before the

House Homeland Security Committee

March 13, 2013

AMERICAN CIVIL LIBERTIES UNION

WASHINGTON LEGISLATIVE OFFICE

915 15th Street, NW Washington, D.C. 20005

(202) 544-1681 Fax (202) 546-0738

Good morning Chairman McCaul, Ranking Member Thompson, and Members of the Committee. Thank you for the opportunity to testify on behalf of the American Civil Liberties Union (ACLU), its more than half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide, about the role of the Department of Homeland Security (DHS) in protecting the cybersecurity of critical infrastructure.

The topic of today's hearing is very timely. DHS is currently the lead agency running major cyber programs on behalf of the government and critical infrastructure, but Congress is considering establishing a new information-sharing regime that could collect cyber information notwithstanding any of the privacy laws currently protecting Americans' sensitive and personal data, and some proposals are unfortunately questioning the role of DHS. Most Americans would agree that the enhancement of online security is a worthy and appropriate goal for those vested with the responsibility for safeguarding the interests of all Americans. Protecting the right to internet privacy – a right with roots in our constitutional principles opposing unreasonable search and seizure and assuring limited government - is as critical a goal as enhancing online security, and DHS is the agency best positioned to handle such new authority in an effective and accountable manner. We look forward to working with this Committee to ensure that these new cyber programs remain under civilian, rather than military control, and that Congress conducts extensive oversight of all DHS programs to ensure protection of privacy rights.

Cybersecurity programs can and must be run in accordance with the Constitution and American values.[1] The internet is an incredibly useful and empowering tool that enhances public knowledge, broadens the reach of our free speech rights, and eases and facilitates daily business and personal activities. As a result, internet data is rich in intimate details of our private and professional lives, such as where we go, with whom we associate, what we read, our religious faith, political leanings, financial status, mental and physical health and more. Protecting privacy is necessary for the public to feel confident in continuing to engage with new and developing technology; any cybersecurity initiatives should make protecting that privacy a paramount goal.

[1] The American Civil Liberties Union's letters to Congress, comments to federal agencies, blogs and other cybersecurity materials may be found at http://www.aclu.org/cybersecurity.

Many existing and proposed cyber efforts do not threaten the privacy or civil liberties of every day internet users, and we urge this Congress and the administration to pursue those programs and to avoid alternative proposals that risk creating major new and unnecessary surveillance programs. Appropriate programs for congressional or administrative action include those to secure government and military networks, educate the public on hygiene issues, prosecute internet-based financial crimes, invest in research and development, secure the supply chain of hardware, and share targeted threat information with critical infrastructure.

I. The Importance of Keeping Domestic Cybersecurity Programs within Civilian Agencies

Under longstanding American legal requirements and policy traditions, the military is restricted from targeting Americans on American soil. Instead, domestic intelligence and law enforcement activities are run by civilian authorities. Some are now arguing that cybersecurity should be the exception, and that military agencies like the National Security Agency (NSA) should be empowered to collect more information about every-day American internet users in order to respond to online threats. Doing so would create a significant new threat to Americans' privacy, and must be avoided.

To date, the military vs. civilian debate has been skewed by the intense focus on cybersecurity threats posed by hostile foreign governments, or international terrorists, and the comparative inattention to threats unrelated to national security. While advanced persistent threats from foreign actors are real and require a multifaceted response from the government, it does not follow that all cybersecurity incidents impacting domestic internet users should merit a military response. Even by intelligence community estimates, those dangers represent a small portion of the threats that affect American internet users. Malware, financial crimes and other threats that do not rise to the level of international incidents make up the overwhelming majority of malicious conduct on the internet. The conflation of foreign spying and potential sabotage, with corporate espionage, everyday internet crime, political statements and essentially prank behavior has inflated every internet malfeasance into a potential national disaster. This hyperbole is simply not factually accurate, and only serves to encourage policy decisions with serious privacy and civil liberties implications.[2]

Placing cyber programs under the jurisdiction of domestic civilian agencies like DHS has real and far more positive consequences for transparency and accountability. DHS's lead competition for cyber programs – the NSA-- is a black hole of information. Programs housed there, like in the rest of the intelligence community, are not subject to any meaningful public oversight. The NSA's activities appear to be presumptively classified, and whatever oversight

[2] See, for example, Howard Schmidt, *Price of Inaction Will Be Onerous*, NYT, Oct. 18, 2012, *available at* http://www.nytimes.com/roomfordebate/2012/10/17/should-industry-face-more-cybersecurity-mandates/price-of-inaction-on-cybersecurity-will-be-the-greatest.

that takes place is cabined in the Intelligence Committees, which conduct most of their business behind closed doors.

One only need look to intelligence wiretapping for an example of the dangers posed if Congress hands control over domestic cybersecurity to the NSA. In 1978, Congress established the Foreign Intelligence Surveillance Act (FISA) to govern foreign intelligence electronic surveillance. Federal judges meeting in a secret court issued opinions interpreting Americans' constitutional rights and developed a secret body of law that the American public has not been allowed to read. The extreme secrecy around such intelligence programs helped conceal a program of illegal and warrantless wiretapping for over six years. Congress eventually amended the FISA to permit this warrantless surveillance to continue, but included a sunset provision that was scheduled to expire at the end of last year. Congress reauthorized it without having a single open hearing with administration witnesses to explain how this expansive authority affects Americans' privacy. While some claim this evolution of expanded wiretapping as a success of the intelligence oversight process, it reflects the limits and consequences of housing these programs behind the intelligence wall.[3]

If cybersecurity – with a set of programs dominated by non-military and non-national security concerns - is ceded to the NSA, this Committee, rank and file members of Congress, and the American public will never hear of it again. Keeping cybersecurity within DHS and other civilian agencies, and within the jurisdiction of this Committee would enhance, not harm, both security and privacy.

II. The Current Role of the Department of Homeland Security in Cybersecurity

Developments over the last several years have rightly steered domestic programs into the DHS or other civilian agencies. In 2010, the Secretary of DHS and the director of the National Security Agency (NSA) signed an agreement that put DHS in charge of cybersecurity in the U.S., with the NSA providing support and expertise.[4] The President's recent Executive Order 13636 continues this approach, putting DHS and the National Institute of Standards and Technology atop the domestic cyber hierarchy, with consultation from the Attorney General, the Privacy and Civil Liberties Oversight Board, and the Office of Management and Budget.[5] These major structural and policy commitments add to longstanding DHS programs that share information with companies and infrastructure operators, educate the public, and secure government systems.

---

[3] The Supreme Court recently ruled in Amnesty v. Clapper that ACLU clients lacked standing to challenge the FISA Amendments Act of 2008, because they could not prove that surveillance of their communications under the act was "certainly impending," all but foreclosing meaningful judicial review of that statute's constitutionality..

[4] MEMORANDUM OF AGREEMENT BETWEEN THE DEPARTMENT OF HOMELAND SECURITY AND THE DEPARTMENT OF DEFENSE REGARDING CYBERSECURITY, September 27, 2010, *available at* http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.

[5] Executive Order 13636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11739, February 12, 2013 [hereinafter Executive Order].

DHS's role in the collection, use, and dissemination of cybersecurity information has substantially grown over the last several years. With the recent executive order, its participation will expand again, especially in two areas. First, DHS will run the Enhanced Cybersecurity Services program and facilitate the sharing of threat indicators with critical infrastructure owners and operators.[6] Information sharing in this direction – from government to private sector – has far fewer privacy implications than the reverse. It does however cement DHS' role in information sharing and publicly available Privacy Impact Assessments suggest that the agency is imposing meaningful privacy protections for the personally identifiable information (PII) coming into its possession. For example, PII is not maintained in a system of records, and therefore is not searchable by name or other identifiers, and information is not retained unless it is "directly relevant and necessary" to address a cyber threat.[7]

Second, DHS will coordinate a review of current information sharing programs to determine whether they meet the ideas in the Fair Information Practice Principles (FIPPs).[8] Currently, there is little publicly available information about what agencies are currently doing with cybersecurity information and this annual report will be the first overarching review of these programs.

III. Emerging Domestic Information Sharing Programs Must Be Run By Civilian Agencies Such as DHS

Congress is considering a significant expansion of the government's authority to collect cybersecurity information, and if the expansion moves forward, it is critical for civil liberties that they be run by civilian agencies such as DHS. H.R. 624, the Cyber Intelligence and Sharing Protection Act (CISPA), would exempt cybersecurity information sharing from all privacy laws and reverse decades of statutory protections for sensitive information like our communication, financial, and internet information. It would permit corporations to determine what information pertains to cybersecurity and allow them to share it with the government – including military agencies like the NSA - and other corporations without making a reasonable effort to shield or scrub out personally identifiable information that is unnecessary to address the threat at hand. Companies would then be free to use Americans' sensitive private information as they see fit, and the government could use it for certain reasons other than cybersecurity. When one of those reasons – national security – is wholly undefined, we are especially concerned that the military and intelligence agencies accessing that information would consider themselves to have free reign over such private records, under ever expanding arguments of what national security includes. These and other fundamental problems are why the ACLU continues to oppose CISPA.

---

[6] *Id*. at 4(c).

[7] PRIVACY IMPACT ASSESSMENT FOR ENHANCED CYBERSECURITY SERVICES, January 16, 2013, *available at* http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf, at 7.

[8] Executive Order at (5).

One of the biggest problems with CISPA is that it does not require companies that participate in this new information sharing regime to work with civilian agencies, and instead allows them to share sensitive and personal information directly with the NSA and other military agencies. The bill's sponsors claim that American corporations insist on dealing with the NSA and may withhold this information from the government altogether if directed to go elsewhere. This assertion does not stand up, especially considering that the companies in question are not part of the defense sector, and primarily offer services to the public and the private sector. Companies that actually have defense information are already permitted to participate in a NSA-run information regime, and other potentially targeted sectors can continue to work with the agencies that have long regulated them.

CISPA insists on giving the companies the authority to share domestic, civilian internet information directly with the NSA even though it neither wants nor needs it. NSA Director General Keith Alexander has stated that his agency should not be the public face of cybersecurity and does not need to directly receive domestic cyber information.[9] In fact, the House Intelligence bill is an outlier. The administration's Statement of Administration Policy on CISPA in the 112th Congress, said that the bill

> …effectively treats domestic cybersecurity as an intelligence activity and thus, significantly departs from longstanding efforts to treat the Internet and cyberspace as civilian spheres. The Administration believes that a civilian agency – the Department of Homeland Security – must have a central role in domestic cybersecurity, including for conducting and overseeing the exchange of cybersecurity information with the private sector and with sector-specific Federal agencies.[10]

The Senate's most recent information sharing legislation, Title VII of the Cybersecurity Act of 2012, also made clear that cybersecurity information should only go to a civilian

---

[9] Jennifer Martinez, *General: Nation Needs DHS Involved in Cybersecurity*, THE HILL, Oct. 21, 2012, *available at* http://thehill.com/blogs/hillicon-valley/technology/259547-general-nation-needs-dhs-involved-in-cybersecurity-, ("I see DHS as the entry point for working with industry," [General Keith] Alexander said at an event hosted by the Wilson Center and National Public Radio…Alexander stressed that protecting the nation's critical infrastructure requires a team effort from the government, including the involvement of DHS. "Where I sit, it's our job to help them be successful. I think they're taking the right steps and it's the right thing to do," Alexander said. "Our nation needs them to be in the middle of this."); Kim Zetter, *DHS, Not NSA Should Lead Cybersecurity, Pentagon Official Says*, WIRED, Mar. 1, 2012, *available at* http://www.wired.com/threatlevel/2012/03/rsa-security-panel/ ("'Obviously, there are amazing resources at NSA, a lot of magic that goes on there,' said Eric Rosenbach, deputy assistant secretary of Defense for Cyber Policy in the Department of Defense. 'But it's almost certainly not the right approach for the United States of America to have a foreign intelligence focus on domestic networks, doing something that throughout history has been a domestic function.' Rosenbach, who was speaking at the RSA Security conference in San Francisco, was adamant that the DHS, a civilian agency, should take the lead for domestic cybersecurity, with the FBI taking a strong role as the country's domestic law enforcement agency.").

[10] OFFICE OF MANAGEMENT AND BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, STATEMENT OF ADMINISTRATION POLICY, H.R. 3523, CYBER INTELLIGENCE SHARING AND PROTECTION ACT, April 25, 2012, *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/112/saphr3523r_20120425.pdf.

agency.[11] While a handful of amendments to CISPA passed on the House floor last year, none of them addressed this point. Members of the Intelligence and Homeland Security Committees filed amendments that would have required new domestic information sharing to be routed through civilian agencies, but they were not made in order and did not receive a vote.[12] The administration, the Senate, and the privacy community are in agreement that civilian control of these programs is not only good for civil liberties, but workable from a cyber and national security standpoint. CISPA stands alone in failing to follow this common wisdom.

IV. Further Areas for Committee Oversight of DHS Cybersecurity

Because of the House's imminent efforts to expand information sharing and the importance of keeping those programs in civilian hands, this statement has focused on that proposal and how it fails from a civil liberties and privacy perspective. But we also urge this Committee to undertake oversight activities of existing cybersecurity programs. In particular, we urge the Committee to review the implementation of the EINSTEIN program, which works with providers to scan government systems for known cyber threats. The last Privacy Impact Assessment on EINSTEIN was written in 2010 and there is little public information about the broader application of the program and the effectiveness of privacy requirements. The Committee should also make sure that agencies are participating meaningfully in the FIPPs review discussed above so that DHS can do an overarching analysis of whether privacy is protected in current programs.

V. Conclusion

Thank you for the opportunity to share our views on cybersecurity and the role of DHS. The administration is giving DHS increasing responsibilities in this area and we hope that if information collection programs expand, they too are housed in DHS. We look forward to working with you on this and other civil liberties issues in the future.

---

[11] S. 3414, The Cybersecurity Act of 2012, 112th Cong. (2012).

[12] CISPA amendments filed with the with the House Rules Committee are available at http://rules.house.gov/Legislation/legislationDetails.aspx?NewsID=812. Amendment 19 by House Permanent Select Committee on Intelligence member Representative Jan Schakowsky (D-IL) and amendment 21 by House Homeland Security Committee Ranking Member Bennie Thompson (D-MS) would have ensured that new sharing under CISPA would have gone to civilian agencies and DHS respectively.