FACILITATING CYBER THREAT INFORMATION SHARING AND PARTNERING WITH THE PRIVATE SECTOR TO PROTECT CRITICAL INFRASTRUCTURE: AN ASSESSMENT OF DHS CAPABILITIES

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

MAY 16, 2013

Serial No. 113–17

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

85–613 PDF WASHINGTON : 2013

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

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan, *Vice Chair*
PATRICK MEEHAN, Pennsylvania
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
JASON CHAFFETZ, Utah
STEVEN M. PALAZZO, Mississippi
LOU BARLETTA, Pennsylvania
CHRIS STEWART, Utah
RICHARD HUDSON, North Carolina
STEVE DAINES, Montana
SUSAN W. BROOKS, Indiana
SCOTT PERRY, Pennsylvania
VACANCY

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
YVETTE D. CLARKE, New York
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
RON BARBER, Arizona
DONDALD M. PAYNE, JR., New Jersey
BETO O'ROURKE, Texas
TULSI GABBARD, Hawaii
FILEMON VELA, Texas
STEVEN A. HORSFORD, Nevada
ERIC SWALWELL, California

GREG HILL, *Chief of Staff*
MICHAEL GEFFROY, *Deputy Chief of Staff/Chief Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

PATRICK MEEHAN, Pennsylvania, *Chairman*

MIKE ROGERS, Alabama
JASON CHAFFETZ, Utah
STEVE DAINES, Montana
SCOTT PERRY, Pennsylvania
VACANCY
MICHAEL T. MCCAUL, Texas *(ex officio)*

YVETTE D. CLARKE, New York
WILLIAM R. KEATING, Massachusetts
FILEMON VELA, Texas
STEVEN A. HORSFORD, Nevada
BENNIE G. THOMPSON, Mississippi *(ex officio)*

ALEX MANNING, *Subcommittee Staff Director*
DENNIS TERRY, *Subcommittee Clerk*

CONTENTS

FACILITATING CYBER THREAT INFORMATION SHARING AND PARTNERING WITH THE PRIVATE SECTOR TO PROTECT CRITICAL INFRASTRUCTURE: AN ASSESSMENT OF DHS CAPABILITIES

Thursday, May 16, 2013

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 9:05 a.m., in Room 311, Cannon House Office Building, Hon. Patrick Meehan [Chairman of the subcommittee] presiding.

Present: Representatives Meehan, Clarke, Vela, Horsford, and Thompson.

Also present: Representative Jackson Lee.

Mr. MEEHAN. The Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will come to order. The subcommittee is meeting today to examine the Department of Homeland Security's National Cyber and Communications Integration Center, better known as the NCCIC, and its capabilities to protect critical infrastructure from cyber attack.

I would like to welcome everybody to today's hearing, which will give Members an opportunity to examine in-depth the work of the Department and Homeland Security's National Cybersecurity Communications and Integration Center.

The NCCIC is one of the U.S. Government's key civilian interfaces with the private sector for cyber-threat information sharing, incident response, and protecting the U.S. critical infrastructure. The NCCIC is a collaborative method for Federal agencies, State and local governmental entities, the private sector, all to communicate cyber-threat information, analysis, and prevention methods in real time.

The subcommittee has been crafting a body of work that will help establish key areas where we can improve the Department's critical infrastructure protection from cyber attack. We have examined the threat, particularly from nation states. We have looked at protecting U.S. citizens from civil liberty violations. Today we look at the threat mitigation capabilities at the Department of Homeland Security.

The director of the National Intelligence, James Clapper, testified before Congress this year, stating that cyber is the No. 1 National security threat facing our country. On March 12, Director Clapper stated, and I quote: "We assess that highly networked business practices and information technology are providing opportunities for foreign intelligence and security services, trusted insiders, hackers, and others to target and collect sensitive United States National security and economic data."

In addition, the director for the National Security Agency, General Keith Alexander, has said that cyber espionage has caused the "greatest transfer of wealth in history."

Our Nation is in a new era and our security is no longer protected by oceans and borders. Indeed, American achievement in the 21st Century will be intricately tied to our ability to secure our networks, primarily our critical infrastructure networks.

While our military protects our Nation from foreign adversaries, the security of our critical infrastructure—our economy, our roads and bridges, domestic energy, water and public utility systems—must be a collaborative effort between the private sector, the local, State, and Federal Government. We need a civilian agency to facilitate this partnership, and that agency is the Department of Homeland Security.

Today's hearing will give us an opportunity to hear from our expert panel regarding ways the NCCIC currently brings a collaborative, National response to cybersecurity. Our capacity within the Committee on Homeland Security is to provide proper oversight to ensure that the NCCIC is functioning properly and is capable of leading in the protection of Federal agencies in cyberspace; it is capable of partnering with critical infrastructure owners and operators to share information and reduce risk; and providing the necessary intelligence elements to assure that State and local critical infrastructure operators are mitigating cyber threats and, I would add, responding appropriately in the aftermath of any kind of activity.

I am looking forward to hearing from our witnesses, particularly in areas that will help the committee as legislators strengthen the Department's capabilities.

We must examine ways to encourage increased participation from owners and operators of critical infrastructure, many of those—most of it—in the private sector. We need to ensure the Department is successfully disseminating threat data with other Federal agencies—in particularly, the Department of Justice and Defense. Most importantly, we must make sure that there are sufficient privacy protections in place to ensure that the Department is able to anonymize data for both personally identifiable information and stakeholder identifiable information.

I look forward to hearing from our panel.

The Chairman now recognizes the Ranking Member of the overall Committee on Homeland Security, Mr. Thompson.

Mr. THOMPSON. Thank you, Mr. Chairman. Thank you for holding today's hearing.

I also want to thank the witnesses for testifying here today.

Over the past few years the cybersecurity mission of the Department of Homeland Security has undergone an unprecedented ex-

pansion in funding and a change in organizational structure. Today I look forward to hearing the testimony from some of the officials responsible for implementing these expanded programs and activities and overseeing the change in the organizational structure and culture.

I also look forward to hearing about how these changes will assist DHS in its efforts to become, in perception and reality, the civilian lead for cybersecurity in the Federal sector. Though once in doubt, it now appears that DHS is bringing together the necessary elements to solidify its leadership role.

In support of these efforts, last month Chairman McCaul and I sponsored an amendment to cyber information-sharing legislation, CISPA, that would establish a center within DHS as the Federal hub for information sharing. I hope this amendment sent a clear signal that any cybersecurity legislation passed by Congress during this session should have a strong role for DHS as a Federal leader in areas where Government and the private sector must work together to prevent cyber attacks and mitigate their impacts.

Today, I want to hear more about DHS's human capital resources. It is my understanding that DHS, like all Federal agencies, is suffering from a shortage of cyber personnel.

As DHS works to ensure its role as a Federal lead for domestic cybersecurity, we cannot ignore our Nation's ability to prepare for, respond to, and recover from advanced cyber threats in a forward-looking endeavor that cannot succeed without sufficient, qualified personnel. We cannot rely on other countries to develop our cyber workforce.

While we cannot predict what cyber threats may occur, we can certainly be prepared and be ready. Be prepared and be ready is a philosophy DHS encourages the public to adopt for natural disasters. Yes, when the oncoming disaster may be a man-made cyber threat, the Department seems to have adopted a "let tomorrow take care of itself" philosophy. Surely this is not acceptable.

DHS must adopt a preparedness philosophy in all aspects of its work. In the world of cyber threats, a part of preparation must be capacity-building programs that include education, outreach, and awareness initiatives.

This year, as hundreds of millions of dollars are poured into Einstein and continuous diagnostic programs, the administration's budget request slashed funding for National initiative for cybersecurity education by $4.8 million, cutting the program by one-third. These cuts will delay efforts to provide cyber outreach and education to 1.7 million high school students.

We cannot continue to complain about the lack of skilled cybersecurity professionals in the American workforce if we are willing to allow DHS to cut the funding it uses to develop the cyber workforce. Again, let me say: We cannot rely on other countries to develop our cyber workforce.

Mr. Chairman, I look forward to hearing from the witnesses and hope that we can work together to restore this funding and ensure that DHS is properly building a defense-in-depth strategy to protect the Nation far into the future.

I yield back.

Mr. MEEHAN. Let me thank the gentleman from Mississippi.

Let me also let the other Members of the committee appreciate that opening statements may be submitted for the record, and we are pleased today to have a distinguished panel of witnesses before us on this very, very important topic.

[The statement of Ranking Member Clarke follows:]

STATEMENT OF RANKING MEMBER YVETTE D. CLARKE

MAY 16, 2013

After a significant expansion of the Department of Homeland Security's cybersecurity mission and programs, beginning in fiscal year 2012, I am glad that we are finally holding a hearing to look at these programs in depth and to assess the progress of the Department in carrying out that mission.

This is the subcommittee's third hearing on cybersecurity this Congress—first, we held a hearing on the threats in cyberspace to our critical infrastructure from state and non-state actors. Next, we learned about how DHS protects the privacy of our citizens in cyberspace.

And with that background in place, today we will hear from the witnesses about whether the Department has the people, programs, and resources in place to successfully address the significant cyber threats to our critical infrastructure while protecting privacy. It is high time that our subcommittee takes a closer look at these programs, some of which did not even exist just a few years ago.

The continuous diagnostics and EINSTEIN programs, in particular, have undergone rapid expansion, and I am pleased that the Department is fulfilling its role as the protector of the dot-gov domain, with the resources to match. But though these Federal network security programs get the majority of the funding and attention, I believe the Department's responsibilities for protecting critical infrastructure, most of which is found in the private sector, is equally important.

For this reason, I am particularly pleased that we are joined by Deputy Inspector General Charles Edwards, who can discuss recent work done by the OIG to assess the progress that ICS–CERT has made to brand itself as the Cyber 9–1–1 for critical infrastructure before, during, and after cyber incidents.

ICS–CERT, recently incorporated as an operational arm of the NCCIC, has done great work in mitigating cyber risks to critical infrastructure, and I look forward to learning more about this mission and the challenges that still remain to share information with the private sector quickly and efficiently.

Finally, I want to register my concerns over the continuing drain of senior cybersecurity leadership at the Department, a trend that has gotten particularly bad in the last 6 months, with the departures of the assistant secretary and the deputy under secretary.

We have been hearing about the difficulties DHS faces in attracting and retaining skilled junior and mid-level cyber employees for a long time, but what does it say about the Department's cyber organization when it cannot retain its senior leaders, either? Rumors are circulating about future replacements for these losses, and I am sure DHS would like to make a splash with these appointments, getting leaders who command respect in the information security and critical infrastructure worlds. But most of all, DHS needs to find leaders who believe in the mission and will stay on board as a steady hand on the wheel during this period of immense expansion and evolution of our cybersecurity efforts.

As part of this process, I believe DHS needs to do some soul-searching and identify why their senior officials have been leaving, and if changes need to be made to ensure future leaders will be more empowered to do their job, I expect that the Department will do so. I hope to work with the Department in this endeavor to guarantee that the vital cybersecurity mission gets the leadership it needs.

Mr. MEEHAN. I have had the chance to visit the NCCIC and to see the great work that is done there, and to listen first-hand to the explanation of what they do, and as a result, it is a great privilege for us today to have the people who are at the front end of that.

First, Ms. Roberta Stempfley is the acting assistant secretary of the Office of Cybersecurity and Communications, where she plays a leading role in developing the strategic direction of the cyber communications and security. A lot of the problem is you have got

to figure out all of these letters in operating things, but it oversees five strategic divisions.

She has previously served as the deputy assistant secretary for the CS&C and as the director of the National Cybersecurity Division. Prior her to work at the CS&C, Ms. Stempfley served as the chief information officer for the Defense Information Systems Agency, where she was responsible for supporting the director in decision making, strategy development, and communication, and management of information technology resources at that agency.

Mr. Larry Zelvin is the director of the National Cybersecurity and Communications Integration Center, the NCCIC, which is housed at the Department of Homeland Security. The NCCIC is comprised of several components, including the U.S. Computer Emergency Readiness team, the National Coordination Center for Telecommunications, the Industrial Control Systems Cyber Emergency Response team, and a 24/7 operations center. Mr. Zelvin is a retired U.S. Navy captain and naval aviator with 26 years of active service.

Mr. Charles Edwards is the deputy inspector general of the Department of Homeland Security. Mr. Edwards is the head of the Office of Inspector General, a role he first attained when named acting inspector general in February 2011. Mr. Edwards has over 20 years of experience in the Federal Government and has held leadership positions at several agencies, including the TSA, United States Postal Office, Inspector—the Office of the Inspector General, and the United States Postal Service.

The witnesses' full written statements appear in the record, and I know that Ms. Stempfley and Mr. Zelvin have offered a joint statement.

So the Chairman now recognizes Ms. Stempfley for 5 minutes to testify, but I do want you to make sure that you hit the important points you have in your testimony. So thank you, Ms. Stempfley. The Chairman now recognizes you for your testimony.

STATEMENT OF ROBERTA STEMPFLEY, ACTING ASSISTANT SECRETARY, OFFICE OF CYBERSECURITY AND COMMUNICATIONS, U.S. DEPARTMENT OF HOMELAND SECURITY, ACCOMPANIED BY LARRY ZELVIN, DIRECTOR, NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. STEMPFLEY. Thank you very much, Chairman Meehan, Ranking Member Thompson, and distinguished Members of the committee. I appreciate the time you have taken today and it is certainly our pleasure to appear before you to discuss the Department of Homeland Security's National Cybersecurity and Communications Integration Center and its role in protecting critical infrastructure from cyber attacks, securing our Federal networks, and coordinating cybersecurity information sharing with the private sector.

Before I begin, I want to thank you for your leadership, sir—Mr. Thompson commented in his opening statement, as well—during the recent legislation debate over the Cyber Intelligence Sharing and Protection Act, and especially in supporting the passing of that

amendment designating DHS as the lead civil Federal entity to receive cyber threat information.

Cybersecurity puts the confidentiality, integrity, and availability of critical services at risk. DHS, along with its Government and private-sector partners, work to counter these threats while supporting a cyber ecosystem that is open, transparent, and less vulnerable to manipulation. The NCCIC supports this effort by providing comprehensive and robust information sharing, incident response, technical assistance, and analysis capabilities to and with our private sector, Government, and international partners. While coordinating with these partners, our goal is to ensure that privacy, confidentiality, civil rights, and civil liberties are not diminished by our security initiatives.

The Department's transparency and public accountability allow us to act as a pipeline to get cyber threat information in the hands of critical infrastructure owners and operators. We are able to share experiences and trends with law enforcement and intelligence communities while preventing malicious actors from gaining access to sensitive sources and methods.

Within DHS's National Protection and Programs Directorate, the Office of Cybersecurity and Communications focuses on managing the risk to communications and information technology infrastructures and the sectors that depend on them. Our role is to enable timely response and recovery of these infrastructures under all circumstances.

The Department manages and facilitates cybersecurity information-sharing efforts, analysis, and incident response activities through the NCCIC. It is a round-the-clock organization where Government, private-sector, and international partners work together towards a whole-of-Nation approach to address cybersecurity and communications issues at the operational level.

We thank those of you who have come out for a tour and invite those who have yet to to do so to come and see the center in operation, with our private-sector partners shoulder-to-shoulder with us in the capabilities.

The NCCIC has experienced over the last year a 68 percent increase from 2011 to 2012 in incidents reported. In 2012 we received 190,000 cyber incidents reported to the NCCIC.

Recently we have been working with the Departments of State, Justice, Treasury, and other interagency partners as well as our industry partners, such as the Financial Services Information Sharing and Analysis Center, to respond to the series of denial-of-service attacks against our financial services industry that have occurred over the past few months. US–CERT has worked, along with the FBI and other interagency partners, to provide technical data, on-site assistance, classified and unclassified briefings in order to help financial institutions and their information technology service providers improve their defensive capabilities.

In addition to sharing with the private-sector entities, we have provided this information to over 120 international partners, many of whom have contributed to the mitigation efforts. These efforts have not only helped financial institutions blunt the impact of these attacks, but have helped the industry develop new strategies

that DHS is sharing with other sectors of critical infrastructure should they face similar attacks.

The Industrial Control Systems Computer Emergency Response—Cyber Emergency Response Team's mission is to reduce the risk to the Nation's critical infrastructure and the control systems that operate within it by strengthening those control systems. We have responded to almost 200 incidents over the last year with 89 on-site visits and 15 teams deployed jointly with the US–CERT to assist in significant private-sector engagements.

In March 2012, the Control Systems—the ICS–CERT identified a campaign of cyber intrusions targeting natural gas pipeline sector with spear phishing e-mails that dated back to December 2011. Responding quickly, we immediately began an action campaign with the Department of Energy and other partners to conduct classified and unclassified briefings across the country providing warnings and mitigation. These entities have been very—have benefitted from this rapid information sharing.

The third entity in the NCCIC is the National Coordination Center for Telecommunications. It leads and coordinates initiation, restoration, and reconstitution of National security emergency preparedness telecommunication services under all conditions.

It has recently collaborated with industry in response to Hurricane Sandy, which enhanced wireless coverage to emergency responders providing emergency services to the 33,400 citizens in Long Beach, New York, the 1.4 million citizens in Nassau County, and the 130,000 citizens in faraway Queens. Their effort supported the recovery of communications to the U.S. financial sector by coordinating fuel and power restoration to key facilities in New York City, ensuring no impact to international financial trading.

The Department's efforts to protect critical infrastructure are enhanced by the recently-issued cybersecurity Executive Order and Presidential Policy Directive on critical infrastructure security and resilience. Both of these documents improve the NCCIC's ability to execute its mission in support of the private sector by strengthening and securing the resilience of critical infrastructure, increasing the role of cybersecurity and securing physical assets, and expanding the coordination and information sharing with critical infrastructure partners.

The Executive Order also supports DHS's strong privacy and civil liberty goals by reinforcing those protections and their incorporation in every aspect of our cybersecurity efforts. The Department believes, however, that the comprehensive suite of cybersecurity legislation is still an essential to improving the Nation's cybersecurity and we are pleased that the administration will continue to work with Congress to achieve this.

Thank you so much for your support and continued attention to this critical issue, and I look forward to your questions.

[The joint prepared statement of Ms. Stempfley and Mr. Zelvin follows:]

JOINT PREPARED STATEMENT OF ROBERTA STEMPFLEY AND LAWRENCE ZELVIN

MAY 16, 2013

INTRODUCTION

Chairman Meehan, Ranking Member Clarke, and distinguished Members of the committee, it is a pleasure to appear before you today to discuss the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC). Specifically, I will discuss the NCCIC's role, responsibilities, and future planning to protect our Nation's critical infrastructure from cyber attacks, secure Federal networks, and coordinate private-sector cyber-threat information sharing.

Before I begin, I would like to thank the committee for its leadership during the recent legislative debate over the Cyber Intelligence Sharing and Protection Act, especially in support of passing an amendment to designate DHS as the lead civilian Federal entity to receive cyber threat information. Cybersecurity threats put the confidentiality, integrity, and availability of critical services at risk. DHS, along with its Government and private-sector partners, works to counter these threats while supporting a cyber ecosystem that is open, transparent, and less vulnerable to manipulation. The NCCIC supports this effort by providing comprehensive and robust information sharing, incident response, technical assistance, and analysis capabilities to private-sector, Government, and international partners.

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 2 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 communicating, traveling, powering our homes, running our economy, and obtaining Government services. No country, industry, community, or individual is immune to cyber risks.

The United States confronts a dangerous combination of known and unknown vulnerabilities in cyberspace and strong and rapidly expanding adversary capabilities. Cyber crime also has increased significantly over the last decade. Sensitive information is routinely stolen from private-sector and Government networks, undermining the integrity of the data contained within these systems. The Department currently sees malicious cyber activity from foreign nations and non-state actors engaged in intellectual property theft and information operations, 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 remote access, thumb drives, supply chain exploitation, and leveraging trusted insiders' access.

The Department has seen motivations for attacks vary from intellectual property theft to criminals seeking financial gain and hackers who may seek bragging rights in the hacker community. Industrial control systems also are targeted by a variety of malicious actors who may have intentions to damage equipment and facilities or steal data. Foreign actors also are 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.

Successful response to dynamic cyber threats requires leveraging homeland security, law enforcement, and military authorities and capabilities, which respectively provide for 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. To achieve a whole-of-Government response, DHS, DOJ, and DOD coordinate continuously to effectively respond to specific incidents. 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."

NCCIC'S CYBERSECURITY MISSION

DHS coordinates the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure by ensuring maximum coordination and partnership with the private sector while ensuring that privacy, confidentiality, and civil rights and civil liberties are not diminished by its security initiatives. Accordingly, the Department has implemented rigorous privacy and civil rights and civil liberties standards, which apply to all of its cybersecurity programs and initiatives. In order to protect privacy while safeguarding and securing cyberspace, DHS institutes layered privacy responsibilities throughout the Department, embeds fair information practice principles into cybersecurity programs and privacy compliance efforts, and fosters collaboration with cybersecurity partners.

Within DHS's National Protection and Programs Directorate (NPPD), the Office of Cybersecurity and Communications (CS&C) focuses on managing risk to the communications and information technology infrastructures and the sectors that depend upon them, as well as enabling timely response and recovery of these infrastructures under all circumstances. CS&C executes its mission by supporting 24×7 information sharing, analysis, and incident response; facilitating interoperable emergency communications; advancing technology solutions for private and public-sector partners; providing tools and capabilities to ensure the security of Federal civilian executive branch networks; and engaging in strategic-level coordination for the Department with private-sector organizations on cybersecurity and communications issues.

To better manage and facilitate cybersecurity information-sharing efforts, analysis, and incident response activities, the Department established the NCCIC, a round-the-clock information sharing, analysis, and incident response center where Government, private-sector, and international partners all work together. The NCCIC is comprised of four branches: The United States Computer Emergency Readiness Team (US–CERT), the Industrial Control Systems Cyber Emergency Response Team (ICS–CERT), the National Coordinating Center for Telecommunications (NCC), and Operations Integration (O&I). As mutually-supporting and integrated elements of the NCCIC, these branches provide the unique authorities, capabilities, and partnerships needed to drive a whole-of-Nation approach to addressing cybersecurity and communications issues at the operational level.

- US–CERT provides advanced information sharing, incident response, and analysis expertise for malicious cyber activity targeting private-sector and Government networks. US–CERT's global partnerships allow it to work directly with analysts from across multiple sectors and international borders to develop a comprehensive picture of malicious activity and mitigation options. US–CERT's mission focuses specifically on computer network defense, and it is able to apply its full resources to supporting prevention, protection, mitigation, response, and recovery efforts.
- ICS–CERT reduces risk to the Nation's critical infrastructure by strengthening the cybersecurity of systems that operate our Nation's critical infrastructure. It carries out this mission by performing incident response to support asset owners with discovery, analysis, and recovery efforts as well as providing situational awareness through training, alerts, and advisories to warn of cyber-based threats and vulnerabilities affecting critical infrastructure assets. In addition, ICS–CERT conducts assessments and technical analysis of malware, digital media, system vulnerabilities, and emerging exploits and partners with the control systems community to coordinate risk management activities.
- NCC leads and coordinates the initiation, restoration, and reconstitution of the National Security/Emergency Preparedness (NS/EP) telecommunications services or facilities during any human-caused or natural event where physical communications infrastructure is damaged or vulnerable. NCC leverages partnerships across Government, industry, and international partners to gain situational awareness and determine priorities for protection and response. NCC's presence in the NCCIC allows DHS to synchronize operational processes supporting both the physical and the virtual components of our Nation's information and communications technology infrastructure.
- O&I applies planning, coordination, and integration capabilities to synchronize analysis, information sharing, and incident response efforts, ensuring effective synchronization across the NCCIC.

STRATEGIC GOALS

The NCCIC works to proactively analyze cybersecurity and communications threats and vulnerabilities and coordinate their findings with partners to manage risks to critical systems; create shared situational awareness among public-sector,

private-sector, and international partners by collaboratively developing and sharing timely and actionable cybersecurity and communications information; and rapidly respond to routine and significant cybersecurity and communications incidents and events to mitigate harmful activity, manage crisis situations, support recovery efforts, and assure NS/EP.

To accomplish its strategic goals, NCCIC relies on the voluntary coordination, collaboration, capabilities, and resources of its partners. The center works closely with those Federal agencies most responsible for securing the Government's cyber and communications systems, including the Departments of Treasury and Energy. The NCCIC also actively engages with the appropriate private-sector entities, information-sharing and analysis centers, State, local, Tribal, and territorial governments, and international partners. As integral parts of the cyberspace and communications community, these groups work together to protect the portions of critical information technology that they interact with, operate, manage, or own. These groups of stakeholders represent natural communities of practice providing the foundation for effective information sharing and response.

Threat Analysis

NCCIC collaborates with private-sector, Government, and international partners to identify, research, and verify suspicious, malicious, or potentially harmful cybersecurity and communications activity, events, or incidents. For example, US–CERT operates NCCIC's Advanced Malware Analysis Center, which receives malware samples and other potentially malicious files from around the world. The Advanced Malware Analysis Center analyzes those files, shares that analysis broadly to alert partners to malicious activity, and provides them with actionable indicators and recommendations to improve their ability to protect themselves.

By understanding the nature of attacks, vulnerabilities, and risks, NCCIC is able to determine possible impacts, set priorities, and proactively develop and share effective mitigation strategies. NCCIC strives to anticipate potentially harmful activity and provide actionable alert and warning information to partners before they are impacted. NCCIC's analysis efforts, whether focused on a new piece of malware or a tropical storm with the potential to damage critical communications systems, contribute directly to its information sharing, response, and protection and prevention capabilities.

Situational Awareness

The success of the NCCIC's mission is heavily reliant on its ability to establish shared situational awareness of potentially harmful activity, events, or incidents across multiple constituencies to improve the ability of diverse and distributed partners to protect themselves. To do this, NCCIC integrates analysis and data received through its own analysis, intelligence community and law enforcement reporting, and data shared by private-sector and international partners into a comprehensive series of actionable information products, which are shared with partners in easy-to-digest machine-readable formats.

Multidirectional sharing of alerts, warnings, analysis products, and mitigation recommendations among Federal, State, local, Tribal, and territorial governments, private sector, including information sharing and analysis centers, and international partners is a key element of NCCIC's cyber and communications protection and prevention framework. The NCCIC continuously works with a broad range of partners to explore and innovate new ways to enhance information sharing and move closer to network speed communications.

Rapid Response

The NCCIC applies the collective capabilities of its partners and constituents to identify, prioritize, and escalate confirmed cybersecurity incidents in order to minimize impacts to critical information infrastructure. To ensure a 24×7 capability, NCCIC maintains cross-functional incident response teams, which draw from the capabilities of NCCIC's branches, along with expertise from elsewhere in DHS such as the United States Secret Service (USSS) and Immigration and Customs Enforcement (ICE). Working under a voluntary request for technical assistance, these incident response teams analyze malware, review network logs, and assess security posture to identify possible malicious activity, its impacts, as well as mitigation and recovery options.

Recognizing the possibility of a cyber incident with physical impacts or a physical incident with cyber implications, NCCIC works increasingly closely with NPPD's National Infrastructure Coordinating Center (NICC). This collaboration, directed by Presidential Policy Directive 21 (PPD–21), helps to ensure strong synchronization between DHS's infrastructure protection efforts in both the cyber and physical realms. In addition, the NCCIC assists in the initiation, coordination, restoration,

and reconstitution of the NS/EP telecommunications services or facilities under all conditions, crises, or emergencies including executing Emergency Support Function 2—Communications responsibilities under the National Response Framework.

These efforts provide a whole-of-Nation approach to incident response, efficiently and effectively leveraging capabilities from across DHS's partner base while implementing key policies.

PROTECTING CRITICAL INFRASTRUCTURE

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 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, and through collaboration between the NCCIC and the NICC, integrates efforts across the physical and cyber domains. The Department also conducts on-site risk assessments of critical infrastructure and shares risk and threat information with State, local, and private-sector partners. NCCIC 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. These efforts provide unique value to private-sector partners by integrating data from companies and industries that might not normally communicate.

In 2011, DHS launched the Cyber Information Sharing and Collaboration Program (CISCP), which is specifically designed to elevate the cyber awareness of all critical infrastructure sectors through close and timely cyber threat information sharing and direct analytical exchange. Through the CISCP, participating private-sector partners are able to share data directly with Government. When requested, these datasets are covered by the Protected Critical Infrastructure Information (PCII) program, which protects the name of the company that shared the information from disclosure through Freedom of Information Act requests, regulatory processes, civil litigation, and other sunshine law requirements. Submitted datasets are analyzed in the context of other data received from across sectors, and based on this analysis regular analytical products are shared back out with partners. CISCP has signed 40 Cooperative Research and Development Agreements (CRADAs), and is in the process of finalizing agreements with 66 additional entities to formalize a streamlined information-sharing process. Since December 2011, CISCP has released over 900 products containing approximately 18,000 cyber threat indicators, which are based on information the Department has gleaned from participant submissions, open-source research, and from sensitive Government information.

NCCIC has also benefited from close collaboration with the USSS and ICE, which have complementary jurisdiction over the investigation of computer crime violations that they exercise to protect the Nation's leaders and critical infrastructure and strategically target transnational organized criminals who are exploiting the financial system through cybercrimes. By working closely together, NCCIC and its law enforcement partners are able to leverage each organization's expertise and unique authorities to more effectively and efficiently execute DHS's cybersecurity mission.

RESPONDING TO CYBER THREATS

As the civilian Department at the intersection of public-private information sharing, DHS is a focal point for coordinating cybersecurity information sharing with the private sector, the Department engages with owners and operators, based on their requests for technical assistance, by providing on-site analysis, mitigation support, and assessment assistance. The Department has repeatedly demonstrated its ability to expeditiously support private-sector partners with cyber intrusion mitigation and incident response. Initiating technical assistance with any private company to provide analysis and mitigation advice is a sensitive endeavor that requires trust and strict confidentiality. DHS's efforts focus on civilian computer network defense and protection rather than law enforcement, military, or intelligence functions in order to mitigate threats to the networks and reduce future risks.

Since 2009, the NCCIC has responded to nearly half-a-million incident reports and released more than 26,000 actionable cybersecurity alerts to the Department's public- and private-sector partners. An integral player within the NCCIC, the US–CERT also provides response support and defense against cyber attacks for Federal civilian agency networks as well as private-sector partners upon request. In 2012,

US–CERT processed approximately 190,000 cyber incidents involving Federal agencies, critical infrastructure, and the Department's 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 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, which includes analyzing data and sharing results, developing mitigation recommendations, and providing alerts and warning to potential future victims. DHS also empowers owners and operators through a cyber self-evaluation tool, the Cyber Security Evaluation Tool (CSET®), which was used by over 1,000 companies last year. In addition, DHS provides in-person and on-line training sessions that focus on network security.

The NCCIC, and its Federal partners, works with the private sector and international partners in preventing intellectual property theft with a whole-of-Government approach. For example, the United States Secret Service—which brings together over 6,000 partners from across sectors through its 29 domestic Electronic Crimes Task Forces (ECTFs)—investigates cyber crimes within its jurisdiction, and the United States Coast Guard contains a component of U.S. Cyber Command and U.S. Strategic Command for the conduct of military missions. In each case, DHS focuses not only on responding to the incident at hand, but also on identifying trends, warning potential victims, and proactively engaging with partners. DHS, in collaboration with FBI and other partners, released a series of Joint Indicator Bulletins, containing cyber-threat indicators to help private-sector partners take action to stop this activity and protect them from theft of intellectual property, trade secrets, and sensitive business information.

Most recently, and in close collaboration with interagency partners as well as industry partners like the Financial Services Information Sharing and Analysis Center, DHS has been engaged with private-sector and international partners during the series of DDoS incidents over the past few months. DHS has provided technical data and assistance, including identifying hundreds of thousands of DDoS-related IP addresses and supporting contextual information in order to help financial institutions and their information technology security service providers improve their defensive capabilities. In addition to sharing with these private-sector entities, DHS has provided this information to over 120 international partners, many of whom have contributed to our mitigation efforts. DHS, along with the FBI and other interagency partners, has also deployed on-site technical assistance to provide in-person support, and has conducted numerous classified briefings on the nature of the threat and mitigation strategies to hundreds of financial-sector IT security specialists. These efforts have helped to increase the U.S. Government's sharing and coordination efforts internally and with private-sector partners. Additionally, the mitigation strategies provided have not only helped financial institutions significantly blunt the impact of these attacks, but they have also helped the industry develop new strategies of their own that DHS hopes to share with other sectors of critical infrastructure to help mitigate similar attacks.

NCCIC's NCC played a vital role in response to Hurricane Sandy recovery efforts. The NCC, as the coordinator for Emergency Support Function No. 2 under the National Response Framework, provided a wide range of communications support in partnership with industry to support responders, citizens, and industry response and recovery. NCC worked to improve first-responder actions by assisting in radio network infrastructure restoration such as microwave connectivity supporting local fire department dispatch and coordination. They also coordinated aid to citizens through more than 170 instances of emergency provisioning of communications installations supporting response organizations such as the American Red Cross, Army Corps of Engineers, Social Security Administration, and the Federal Emergency Management Agency. Collaborating with industry, NCC enhanced wireless coverage to first responders who provide emergency services to approximately 33,400 citizens in Long Beach, New York; 1,400,000 citizens in Nassau County and 130,000 citizens in Far Rockaway, Queens. Their efforts also supported the recovery of communications to the U.S. financial sector by coordinating fuel and power restoration to a key facility in New York City, ensuring no impact to international financial trading.

Finally, in March 2012, DHS identified a campaign of cyber intrusions targeting natural gas pipeline sector companies with spear-phishing e-mails that dated back to December 2011. The attacks were 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 op-

eration of the systems. While there is no evidence that anyone has tried to subvert the operation of these industrial control systems, the intent of the attacker remains unknown. DHS immediately began an action campaign to alert the oil and natural gas pipeline sector community of the threat and offered to provide assistance. Industry partners have been responsive to these threats, and in May and June 2012, DHS deployed on-site assistance to two of the organizations targeted in this campaign: An energy company that operates a gas pipeline in the United States and a manufacturing company who specializes in producing materials specific to pipeline construction. DHS also partnered with the Department of Energy and others to conduct briefings across the country. Over 500 private-sector individuals attended the classified briefings and hundreds more received unclassified briefings providing warnings and mitigation strategies.

RECENT EXECUTIVE ACTIONS

As today's physical and cyber infrastructures become increasingly linked, critical infrastructure and emergency response functions grow ever more 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 marketplace. These policies work in conjunction with Executive Order 13618 of July 6, 2012, Assignment of National Security and Emergency Preparedness Communications Functions, which improves how the Executive branch handles NS/EP Communications and ties cyber into emergency response communications.

In February 2013, President Obama issued EO 13636, as well as PPD–21 on Critical Infrastructure Security and Resilience, which will work to 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, and will improve NCCIC's ability to execute its mission in support of the private sector. The President's actions mark an important milestone in the Department's on-going 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, and these policies will further enable NCCIC's mission. EO 13636 supports more efficient sharing of cyber-threat information with the private sector and directs the National Institute of Standards and Technology to develop a Cybersecurity Framework to identify and implement better security practices among critical infrastructure sectors. EO 13636 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.

EO 13636 also expands the DHS Enhanced Cybersecurity Services (ECS) program, key aspects of which are operated by the NCCIC. ECS is a voluntary information-sharing program that assists critical infrastructure owners and operators to improve protection of their systems from unauthorized access, exploitation, or data exfiltration. DHS works with cybersecurity organizations from across the USG to gain access to a broad range of cyber-threat information. ECS consists of the operational processes and security oversight required to share sensitive and classified cyber-threat information with qualified Commercial Service Providers (CSPs) that will enable them to better protect their customers who are critical infrastructure entities. CSPs can deliver approved services to validated critical infrastructure entities through commercial relationships. The ECS program is not involved in establishing commercial relationships between CSPs and CI entities. ECS augments, but does not replace, entities' existing cybersecurity capabilities. The ECS information-sharing process protects Critical Infrastructure (CI) entities against cyber threats that could otherwise harm their systems. ECS program participation is voluntary and designed to protect Government intelligence, corporate information security, and the privacy of participants, while enhancing the security of critical infrastructure. Validated CI entities from all 16 CI sectors are eligible to participate in the ECS program and receive ECS services from an eligible CSP.

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 calls for a comprehensive research and development plan for critical infrastructure to guide the Government's effort to enhance market-based innovation. The strategic imperatives in PPD–21 also direct the NCCIC and the NICC to "function in an integrated manner and serve as focal points for critical infrastructure partners to obtain situational awareness and integrated, actionable information to protect the physical and cyber aspects of critical infrastructure." As such, NPPD is

enhancing the existing coordination of its two critical infrastructure operations centers, the NCCIC and the NICC.

CONTINUING NEED FOR LEGISLATION

We continue to believe that carefully-crafted information-sharing provisions, as part of a comprehensive suite of cybersecurity legislation, are essential to improve the Nation's cybersecurity to an acceptable level, 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 2 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

Set within an environment characterized by a dangerous combination of known and unknown vulnerabilities, rapidly-evolving adversary capabilities, and a lack of comprehensive threat and vulnerability awareness, the cybersecurity mission is truly a National one requiring broad collaboration. DHS is committed to creating a safe, secure, and resilient cyber environment while promoting cybersecurity knowledge and innovation and protecting privacy, confidentiality, civil rights, and civil liberties in collaboration with its public, private, and international partners. Thank you for your continued support and attention to the critical issue of cybersecurity and I look forward to your questions.

Mr. MEEHAN. [Off mike.]

One of us thinks we have to get technology as my button to work.

Thank you, Ms. Stempfley, for your testimony. As I identified at the outset, Mr. Zelvin joins in that testimony on behalf of the Department of Homeland Security.

So now the Chairman recognizes Mr. Edwards, Inspector General's Office of DHS, for your testimony.

STATEMENT OF CHARLES K. EDWARDS, ACTING INSPECTOR GENERAL, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. EDWARDS. Good morning, Chairman Meehan, Ranking Member Clarke, Ranking Member Thompson, and Members of the subcommittee. Thank you for the opportunity to discuss DHS efforts to secure the Nation's industrial control systems. The majority of information that I will provide is contained in our February 2013 report, "DHS Can Make Improvements to Secure Industrial Control Systems."

Industrial control systems, or ICS, are systems that manage and monitor the Nation's critical infrastructure and key resources, or CIKR. ICS are increasingly under attack by a variety of malicious sources, ranking from hackers looking for attention and reputation to sophisticated nation states intent on damaging equipment and facilities, disgruntled employees, or competitors.

Successful attacks on ICS can give malicious users direct control of operational systems, creating the potential for large-scale power outages or man-made environmental disasters and can cause physical damage, loss of life, and other cascading effects.

DHS has strengthened the security of ICS by addressing the need to share critical cybersecurity information, analysis vulnerabilities, verify emerging threats, and disseminate mitigation strategies. DHS has taken a number of actions to improve ICS se-

curity and foster better partnership within Federal and private sectors.

For example, DHS has established the ICS–CERT Incident Response Team, also known as the fly-away team, to support the public and private sectors through on-site and remote incident response services on a variety of cyber threats. DHS has improved the quality of its alerts and bulletins by including actionable information regarding vulnerabilities and recommended mitigations and best practices for securing ICS. Finally, the Department has strengthened its outreach efforts with the ICS community, including vendors, owners, operators, and academic community and other Federal agencies.

Although DHS has made improvements, more needs to be done to reduce the cybersecurity risks for the Nation's ICS. Many of the private-sector partners we interviewed use portals such as the Homeland Security Information Network, or HSIN, to retrieve advisories, vulnerability information, and best practices. There are 55 communities of interest on the HSIC Critical Sectors portal intended to facilitate communication and collaboration among all CIKR sectors and the Federal Government.

However, DHS does not have a consolidated summary overview page on the HSIN Critical Sectors portal that highlights new information and activities to ensure that ICS cybersecurity information is shared effectively. As a result, the content of each of the CIKR sectors must be searched individually for pertinent and updated information. These searches can be time-consuming for the stakeholders.

In addition, all the sector-specific agencies senior officials that we interviewed expressed a need to be notified in advance when ICS–CERT is performing on-site or remote technical assistant assessments with private companies within their sectors. For example, these officials suggested that ICS–CERT publish a heads-up or a quick anonymous informational alert regarding an on-going investigative or pending event, sectors and devices affected, and whether a potential fix exists. Such notification would be helpful and would allow them to react more accordingly if other companies call them with questions.

Overall, officials acknowledge that DHS had improved the quality of alerts and bulletins that address various cyber topics. However, they expressed concern regarding the timeliness of ICS–CERT's information sharing and communications. ICS–CERT management acknowledged that sector-specific agencies, councils, and private sectors concerning regarding the sharing of active incidents and threats, such as identified cyber intrusions and spear phishing e-mails.

However, proprietary information and on-going law enforcement investigations sometimes limit the amount of information ICS–CERT can disseminate. The report included two recommendations and NPPD concurred with both.

Mr. Chairman, this concludes my prepared remarks, and I would be happy to answer any questions that you or the Members may have.

Thank you.

[The prepared statement of Mr. Edwards follows:]

PREPARED STATEMENT OF CHARLES K. EDWARDS

MAY 16, 2013

Good morning Chairman Meehan, Ranking Member Clarke, and Members of the subcommittee: Thank you for the opportunity to discuss DHS' efforts to secure the Nation's industrial control systems. The majority of information that I will provide today is contained in our February 2013 report, *DHS Can Make Improvements to Secure Industrial Control Systems* (OIG–13–39).

Industrial control systems (ICS) are systems that include supervisory control and data acquisition, process control, and distributed control that manage and monitor the Nation's critical infrastructure and key resources (CIKR).[1] ICS are an integral part of our Nation, and help facilitate operations in vital sectors. Beginning in 1990, companies began connecting their operational ICS with enterprise systems that are connected to the internet. This allowed access to new and more efficient methods of communication, as well as more robust data, and gain quicker time to market and interoperability. However, security for ICS was inherently weak because it allowed remote control of processes and exposed ICS to cybersecurity risks that could be exploited over the internet. As a result, ICS are increasingly under attack by a variety of malicious sources. These attacks range from hackers looking for attention and notoriety to sophisticated nation-states intent on damaging equipment and facilities, disgruntled employees, competitors, and even personnel who inadvertently bring malware into the workplace by inserting an infected flash drive into a computer. A recent survey revealed that a majority of the companies in the energy sector had experienced cyber attacks, and about 55 percent of these attacks targeted ICS. These attacks involved large-scale denial-of-service and network infiltrations. Successful attacks on ICS can give malicious users direct control of operational systems, creating the potential for large-scale power outages or man-made environmental disasters and cause physical damage, loss of life, and other cascading effects that could disrupt services.

Some recent cyber attacks have included the following:

- In February 2011, the media reported that hackers had stolen proprietary information worth millions of dollars from the networks of six energy companies in the United States and Europe.
- In December 2011, a sophisticated threat actor targeted the oil and natural gas subsector. Affected asset owners across the sector voluntarily worked with DHS during the investigation.
- Throughout 2011, there were reports of spear-phishing via email in the energy sector; no negative impacts occurred to the companies' control processes and operations.
- In March 2012, an alert was issued regarding phone-based social engineering attempts at two or more power distribution companies. The callers attempted to direct the company personnel to take action to correct a problem that would have allowed the attacker to gain access to their ICS.
- In April 2012, media reported that a Canadian ICS manufacturing company inadvertently planted a backdoor login account in its own operating systems, which contain switches and servers used in mission-critical communications networks that operate power grids and railway and traffic control systems. This account could have allowed attackers to access the devices via the internet.

The Industrial Control Systems—Cyber Emergency Response Team's (ICS–CERT) operational capabilities focus on the private-sector CIKR ICS and networks, which is essential to the Department's mission to protect the Nation's critical infrastructure, particularly against emerging cyber threats. Additionally, ICS–CERT uses the Request Tracker Ticketing System to capture analytical and status information regarding vulnerabilities and incidents. The ticketing system maintains the incident response team's remote technical assistance and on-site assessment status and reports. Tickets are color-coded based on age. The ticketing system notifies the assigned personnel when the status of a ticket is changed or further action is needed. Additionally, ICS–CERT coordinates control systems-related security incidents and information sharing with Federal, State, and local agencies and organizations, as well as private-sector constituents, including vendors, owners, and operators of ICS.

[1] There are 18 CIKR sectors: Agriculture and Food, Banking and Finance, Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Government Facilities, Healthcare and Public Health, Information Technology, National Monuments and Icons, Nuclear Reactors, Material and Waste, Postal and Shipping, Transportation Systems, and Water.

ICS–CERT exchanges information with stakeholders via the Homeland Security Information Network (HSIN)—Critical Sector. The Office of the Chief Information Officer (OCIO) develops and maintains HSIN and serves as data governance steward for HSIN policy documents, including the HSIN Model Charter and HSIN Terms of Service. Although OCIO is the data steward, the office is not responsible for maintaining the content that users and communities of interest post to any element of HSIN.[2] Each community of interest sponsor is responsible for maintaining and sharing the content within the community of interest and through the community of interest shared space.[3] The administration and governance of the communities of interest, including creation of individual sites within the community, is at the discretion of their sponsors. OCIO works in cooperation with each community of interest to enforce the rules in the charter and terms of services. OCIO conducts regular reviews of communities of interest to validate and justify its purpose, objectives, and operational need. National Protection and Programs Directorate (NPPD) sponsors and manages the critical sector communities of interest.

DHS' PROGRESS IN IMPROVING THE SECURITY OF INDUSTRIAL CONTROL SYSTEMS

We reported that Department needed to improve the security of ICS and information sharing to enhance program effectiveness. DHS has strengthened the security of ICS by addressing the need to share critical cybersecurity information, analyze vulnerabilities, verify emerging threats, and disseminate mitigation strategies. For example, DHS has taken the following actions to improve ICS security and foster better partnerships between the Federal and private sectors:

- Establishing ICS–CERT Incident Response Team, also known as the fly-away teams, to support the public and private sectors through on-site and remote incident response services on a variety of cyber threats, ranging from general malicious code infections to advanced persistent threat intrusions. Additionally, in March 2012, NPPD released the Cyber Security Evaluation Tool Version 4.1. The updated tool assists users in identifying devices connected to their networks, as well as external connections, by creating a diagram of their systems.
- Operating a malware lab that provides testing capabilities to analyze vulnerabilities and malware threats to control system environments. The team verifies vulnerabilities for researchers and vendors, performs impact analysis, and provides patch validation and testing prior to deployment to the asset-owner community.
- Improving the quality of its alerts and bulletins by including actionable information regarding vulnerabilities and recommended mitigations and best practices for securing ICS.
- Providing products to the ICS community on a daily, weekly, monthly, quarterly, and as-needed basis, through email, website, and portal postings. These products help ICS–CERT to improve the situational awareness of ICS and provide status updates of its working groups, articles of interest, and upcoming events and training.
- Implementing a virtual private network solution to allow NPPD program officials to access program applications and systems (e.g., the ICS–CERT ticketing system) located at the Idaho National Laboratory (INL).[4]
- Assisting in developing various roadmaps for the cross-sector, dams, nuclear, water, and transportation. The road maps provide vision and framework for mitigating cybersecurity risk to the wide variety of systems critical to each sector's operations.

Finally, the Department has strengthened its outreach efforts with the ICS community, including vendors, owners/operators, academia, and other Federal agencies. These efforts include participating in the periodic meetings with the Cross-Sector Cyber Security Working Group; Government Coordinating Council and Sector Coordinating Council; and various sector-specific groups.

---

[2] HSIN communities of interest are separate environments wherein users involved in the same subject matter area or industry may post and view potentially relevant news and information and use collaborative tools.

[3] The HSIN shared space allows authorized stakeholders and content contributors to publish finished products and relevant documents that: (1) Have appropriate markings providing sharing permissions at the document level, and (2) are targeted to an authorized audience based on their credentials and related community of interest and system-wide rules for sharing.

[4] A virtual private network is a technology for using the internet or another intermediate network to connect computers to isolated remote computer networks that would otherwise be inaccessible. Users can access resources on remote networks, such as files, printers, databases, or internal websites.

MAJOR CHALLENGES

Despite these actions, NPPD still faces challenges in reducing the cybersecurity risks for the Nation's ICS. Further, NPPD can improve its efforts to protect and secure control systems that are essential to the Nation's security and economy. Specifically, ICS–CERT needs to consolidate its information-sharing and communication efforts with Sector-Specific Agencies and the private sector to ensure that these stakeholders are provided with potential ICS threats and vulnerabilities to mitigate security threats timely. In addition, DHS needs to improve communications with Sector-Specific Agencies and the private sector by providing advanced notification of ICS–CERT's remote technical and on-site incident assessments.

Consolidation of Multiple Information-Sharing Communities of Interest

Many of the private-sector partners we interviewed (e.g., owners/operators, regulators, and working groups) use the HSIN, ICS–CERT, and United States Computer Emergency Readiness Team (US–CERT) portals to retrieve advisories, vulnerability information, and best practices. There are 55 communities of interest on the HSIN–Critical Sectors intended to facilitate communication and collaboration among all CIKR sectors and the Federal Government. However, DHS does not have a consolidated summary overview page on HSIN–Critical Sectors that highlights new information and activities to ensure that ICS cybersecurity information is shared effectively. As a result, the content for each of the CIKR sectors and must be searched individually for pertinent and updated information. For example, the Dams, Emergency Management, and Electricity and Oil and Natural Gas subsector communities of interest, which are used by companies that belong to multiple sectors, have to be searched individually and may contain non-cybersecurity information, such as physical security, emergency response, and planning. These searches can be time-consuming for the stakeholders.

Additionally, each community of interest is arranged differently, making it more cumbersome for the users to retrieve useful information. For example, some HSIN users told us that the various communities of interest contain duplicate information. As a result, some Sector-Specific Agencies want to build additional portals for their stakeholders to streamline the information DHS provides.

ICS–CERT officials acknowledged that existing communities of interest could confuse owners/operators. To eliminate duplicate information from the communities of interest, ICS–CERT created a subcommittee to address stakeholder concerns regarding the communities of interest. ICS–CERT officials said that ICS–CERT only contributed content to the communities of interest and does not have the responsibility for site set up. However, NPPD plans to hold discussions with OCIO to determine whether these communities of interest could be consolidated to better serve stakeholder needs.

We recommended that the Under Secretary, NPPD collaborate with OCIO to streamline the HSIN portal to ensure that ICS cyber information is shared effectively.

Advance Notification of Remote Technical and On-site Assessments

All the Sector-Specific Agencies senior officials that we interviewed expressed a need to be notified in advance when ICS–CERT is performing on-site or remote technical assistance assessments with private companies within their sectors. For example, these officials suggested that ICS–CERT publish a "heads-up" or "quick anonymous" informational alert regarding an on-going investigative/pending event, sectors and devices affected, and whether a potential fix exists. The Sector-Specific Agency officials told us that such notifications would be helpful and would allow them to react more appropriately if other companies call them with questions. For example, according to Nuclear Sector-Specific Agency officials, the Department's Domestic Nuclear Detection Office sends an email alert to State authorities and its offices regarding upcoming site visits.

DHS does not communicate timely the results of its remote technical and on-site assessments to the public. We interviewed officials from three Sector-Specific Agencies, six Government and private-sector councils, and 23 private companies from the dams, energy, and nuclear sectors to evaluate whether ICS–CERT shared sufficient information and communicated effectively. Overall, these officials acknowledged that DHS had improved the quality of alerts and bulletins that addressed various cyber topics. However, they expressed concerns regarding the timeliness of ICS–CERT's information sharing and communications. As a result, the stakeholders are concerned that a great deal of time might elapse until stakeholders were made aware of the same or similar incident that could affect their systems.

Additionally, both Sector-Specific Agencies and private-sector officials said that an advance notification would be helpful to increase dialogue with ICS–CERT on an

event or threat that has not been made public. The private-sector officials suggested that advance notification can allow them to assist ICS–CERT in developing solutions and mitigating strategies as well as determining whether an incident is isolated or systemic.

ICS–CERT management acknowledged the Sector-Specific Agencies', councils', and private sector's concerns regarding the sharing of active incidents and threats, such as identified cyber intrusions and spear-phishing emails. Additionally, ICS–CERT management told us that the private sector perceives that ICS–CERT has more useful information available than it is willing to share. However, ICS–CERT management said that proprietary information and on-going law enforcement investigations limit the amount of information ICS–CERT can disseminate. For example, there were instances in which the Federal Bureau of Investigation was engaged in an on-going investigation and had withheld sensitive law enforcement information. Additionally, the protected critical infrastructure information between DHS and the private-sector owner prohibits ICS–CERT from sharing vulnerability and malware assessment information.

We recommended that the Under Secretary, NPPD promote collaboration with Sector-Specific Agencies and private-sector owners/operators by communicating preliminary technical and on-site assessment results to address and mitigate potential security threats on ICS.

Mr. Chairman, this concludes my prepared statement. I appreciate your time and attention and welcome any questions from you or Members of the subcommittee.

Mr. MEEHAN. Thank you, Mr. Edwards, for your testimony.

Before we go to the opportunity for my colleagues to present their questions to you, I am pleased to be joined by the Ranking Member of our committee, the gentlelady from New York, and I recognize her now for opening comments that she may have?

Ms. CLARKE. Thank you very much, Mr. Chairman, and thank you to the Ranking Member and my colleagues.

Mr. Chairman, I want to thank you once again for holding this morning's hearing. After significant expansion of the Department of Homeland Security's cybersecurity mission and programs beginning in fiscal year 2012, I am glad that this morning we have had the opportunity to examine these programs and are now able to assess the progress of the Department in carrying out the mission.

As you are aware, this is the subcommittee's third hearing on cybersecurity in this Congress. First we held a hearing on the threats in cyberspace through our critical infrastructure from state and non-state actors. Next we learned about the DHS—how DHS protects the privacy of our citizens in cyberspace. With the background in place, today we have heard from the witnesses about the Department and has the—about whether the Department has people, programs, and resources in place to successfully address the significant cyber threats to our critical infrastructure while protecting privacy.

It is high time that our subcommittee take a closer look at these programs, some of which did not even exist just a few years ago. The continuous diagnostics and Einstein programs in particular have undergone rapid expansion, and I am pleased that the Department is fulfilling its role as the protector of the dot-gov domain with the resources to match.

But though these Federal network security programs get the majority of the funding and attention, I believe the Department's responsibilities for protecting critical infrastructure, most of which is found in the private sector, is equally important. For this reason, I am particularly pleased that we have been joined this morning by Deputy Inspector Charles Edwards and that he has discussed the recent work done by the OIG to assess the progress that ICS–

CERT has made to brand itself as the cyber 9–1–1 for critical infrastructure before, during, and after cyber incidents.

ICS–CERT, recently incorporated as an operational arm of the NCCIC, has done great work in mitigating cyber risks to critical infrastructure and it was important that we learned more about this mission and the challenges that still remain to share information with the private sector quickly and efficiently.

Finally, I want to register my concerns about the continuing drain of senior cybersecurity leadership at the Department, a trend that has gotten particularly bad in the last 6 months, with the departures of the assistant secretary and the deputy under secretary. We have been hearing about the difficulties DHS faces in attracting and retaining skilled junior and mid-level cyber employees for a long time, but this—but what does it say about the Department's cyber organization when it cannot retain its senior leaders as well?

Rumors are circulating about the future replacements of these losses, and I am sure DHS would like to make a splash with these appointments, getting leaders who command respect in information security and critical infrastructure worlds. But most of all, DHS needs to find leaders who believe in the mission, that will stay onboard as a steady hand on the wheel during this period of immense expansion and evolution of our cybersecurity efforts.

As part of this process, I believe DHS needs to do some soul searching and identify with why their senior officials have been leaving. If changes need to be made to ensure future leaders will be more empowered to do their job, I expect that the Department will do so. I hope to work with the Department in this endeavor to guarantee that vital cybersecurity mission gets the leadership it needs.

Once again, I would like to thank all of you for testifying before us this morning.

I yield back the balance of my time.

Mr. MEEHAN. I thank the Ranking Member for her opening comments.

We are grateful, again, for your presence here today, of this distinguished panel.

So I now recognize myself for 5 minutes of questioning.

Let me begin by sharing an observation that I believe we in Congress, and in fact, across the Governmental sector, aren't doing a good enough job of really alerting the citizens in general about the true nature and scope of the threat that we face. We often respond in the aftermath of an incident and spend time analyzing what we could have done better.

I believe the work that you are doing is not only vital to the security of our Nation, but you have done some tremendous things in the form of anticipating and sharing and communicating.

So please, if I can just ask Mr. Zelvin and Ms. Stempfley, quickly, what is your assessment of the true nature of the threat that we face today in the world of cybersecurity?

Ms. Stempfley.

Ms. STEMPFLEY. I had to figure the button out, too.

Thank you very much for the opportunity to answer that question. As we have all recognized, cyber pervades almost every facet of our life—we do banking on-line, we do—I renew my driver's li-

cense on-line, our workplace has gone entirely on-line—and a recognition of that important part that the cyber landscape plays in this is certainly not something I think is widely known. So I agree with your point.

We in the Department have been very focused on sharing actionable information, those threat indicators that can be put out there, whether it from a criminal source, whether it come from a hacktivist source, whether it comes from an intelligence source—putting that in the hands of the people who can do the most with it. I know Mr. Zelvin will give you very specific indications of that as he goes through his response to this question.

But we have to pair that with raising the overall understanding of the population of the role that cyber plays, and so some of the other programs that are outside the technology programs that the Office of Cybersecurity and Communication has in things like the "Stop, Think, Connect" campaign and other broad awareness campaigns will raise that—serves to raise that awareness so that consumers can understand what the impact is to them and will live up to some of their obligations, as well.

Mr. MEEHAN. Mr. Zelvin, it is consumers, and Ms. Stempfley focused to some extent on the impact on the everyday American, but it is much broader than that, is it not, with respect to the very infrastructure that we have in this Nation, including our grids and other things of that nature?

Mr. ZELVIN. It is, Mr. Chairman. When I look at the challenge I look at the threats, I look at the victims, and I look at the mitigation capabilities. So as you look at the threats, it is as Ms. Stempfley said, it can affect the individuals.

But there is also nation states. There are also criminal actors. There are nefarious actors and there are just people who want to see if they can do it for the sake of doing it.

When you look at the victims, you have companies that are worth billions of dollars internationally. You have victims such as my aunt, who called me on a weekend and said, "Why is DHS locking my computer and want $400 to unlock it?" She was a victim of something called ransomware. Some virus got on and she couldn't unlock it.

So the victims are very sophisticated or they are an elderly woman who doesn't understand why her computer isn't working.

As you look at the mitigation capabilities, they are also varied. Some companies have magnificent capabilities, and probably we need the Government to provide information and a warning of what is happening and some suggestions on what to do, and then they are off and running and can deal with the challenges.

Other places, they have no capability. They are not sure what to do. They are very confused by the threat and they know it is a problem, but they are not really sure what to do.

In many cases they buy products from the commercial sector—anti-virus vendors—and hope that can be the solution. But it many cases it won't as they are stealing personal identifiable information, potentially financial information.

Mr. MEEHAN. Would you jump off of that point, because I think it gets to the heart of what is so important about the work you do in the NCCIC, and particularly the fact that we have a moldable—

or we have a broad range of capabilities, as you identified, very sophisticated capacities that not only rival but probably work in concert with the capacities—the highest level of capacities that we have in the Government sector, and I am talking about the banking sector, in some ways the communication sector and others.

In other places we have systems that are dramatically behind, and I am talking about things like water systems or other kinds of municipal authorities, but all of which today are tied to the internet, and therefore, the operating systems are capable of being influenced and attacked.

At some point, Mr. Edwards, you have done work into looking at that.

But, Mr. Zelvin, explain the important role that the NCCIC plays in being more or less a junction that is able to tie together the capacity to take the best of what we have and allow it to be available to support those industries which are lagging dramatically behind.

Mr. ZELVIN. Mr. Chairman, as I look at the—you know, you mentioned what is it going to take for people to understand this cyber challenge? I will tell you, there is a variety of experiences, and those who have been attacked the most are obviously the most aware and the most prepared, and that, I think are the financial services sector and the communications sector and the information technology sector. These are the folks that are living and breathing attacks on a daily basis and they are becoming more sophisticated by the day.

There are other sectors, as you mentioned, that haven't had these attacks. So what we do in the NCCIC is we look across the 16 critical infrastructures and we try and raise the water to keep all the boats at the same level, if you will.

So we highlight across the sectors. That is, what is happening in one sector today could be happening in another sector tomorrow. So we want to increase the awareness.

We are also sharing those mitigation strategies. In some cases—in many cases—these are things that companies can do themselves, so we just want to reinforce. There is a friction within the critical infrastructure because in many cases—I apologize—the information technology and the security folks, they are not part of the profit, so—and there is money that needs to be brought into this solution.

So what we try to do is we tell those that are in the leadership position to really listen to these security professionals and really deal with these cyber practices because they can affect your core businesses.

I would also like to mention that we also work with State, local, and Tribal, territorial governments. We work with international partners. There are over 200 countries that we deal with almost on a weekly basis.

So it is the critical infrastructure, it is our State, local, Tribal, territorial, it is our Federal Department's agencies, international, and as I said, the individuals. But the cyber threat is literally global in nature and we are trying to make sure we have awareness and help with the prevention mitigation across the board.

Mr. MEEHAN. Well, my time is expired but I look forward to following up on some of that with the second line of questions.

Now the Chairman recognizes the ranking lady from—the gentlelady from New York, the Ranking Member, Ms. Clarke?

Ms. CLARKE. Thank you, Mr. Chairman.

Ms. Stempfley, I wanted to delve into Einstein 3. DHS has requested large funding increases to build out Einstein 3, which will help prevent intrusions into civilian Federal networks. While I am supportive of this program, I am concerned about the progress of such a large initiative and want to make sure it is carried out properly to ensure that our Federal networks are secured and to keep the cost to the taxpayers down.

A recent report by GCN Magazine raised concerns that Einstein may be over budget and behind in implementation. For the record, can you give the subcommittee an update on Einstein, particularly Einstein 3? What is the schedule for deploying it at all departments and agencies, and do you expect there to be cost and time frame overruns?

Ms. STEMPFLEY. Thank you, ma'am.

Einstein 3 is a part of a comprehensive set of capabilities for perimeter protection known as the National Cybersecurity Protection System. Just about a year ago we transitioned Einstein 3 from being a consolidated, Government-provided hardware and data capability—classified capability to be deployed at the internet service providers—to one that takes advantage of the innovation that the internet service providers can provide into this environment, so that classified Government information and countermeasures can be deployed in an environment where the ISPs, who are most knowledgeable of their own infrastructure and of the ability to transmit traffic, can absorb that and innovate with the Government in this environment.

We are pleased to have notified Congress, I believe 5 weeks ago, of the award of the first of those contracts with CenturyLink, the first internet service provider, and we are in process of transitioning Federal departments onto that capability.

An important piece of information here is that we transition Federal departments who are using that service provider. So we are not asking departments to move from whichever internet service provider provides their connection; we are employing this protection measure in place within that mechanism.

So we are targeting those departments who are—whose service provider is CenturyLink. We are continuing to actively engage with the other four internet service providers for contract award in those instances, and that has been negotiation that is on-going. So we are very happy about that.

We are still on target to reach our final operational capability in the end of 2015. This transition that we made a year ago actually moved our final operational capability from 2018 back to 2015, so we saw that as a very beneficial capability for us to employ this protection across the entire Federal enterprise.

Ms. CLARKE. Fabulous. With that efficiency in time is there an efficiency in cost, as well?

Ms. STEMPFLEY. As it turned out in the analysis, the cost was identical between the two transitions within a small margin. It did not actually save us money but it also did not cost additional money over the life-cycle cost of the program.

Ms. CLARKE. Very well. Thank you for that update.

Mr. Edwards, you released a report just yesterday detailing serious information security deficiencies at CBP. Is this—a little point of departure but I think it is critical when we look at our vulnerabilities.

Some of the—what you outlined in your report is that there are some poor practices, including computers that were not locked or not password protected, a failure to require that employees sign in—or sign nondisclosure agreements for sensitive systems they received access to. Making matters worse, many of these issues had been previously identified by the OIG. Your recommendations based on these findings were directed to the CBP chief information officer and the DHS chief information officer but there is no role for the Office of Cybersecurity Communications within NPPD to play to help the rest of the Department improve their cyber practices.

Could you give us a little more of a sense of what your observations and what this level of vulnerability can mean to the overall cyber environment that we find ourselves in?

Mr. EDWARDS. Thank you, ma'am.

The report that I released yesterday was in reference to the CBP I.T. management letter. Part of the financial statement audit—we use KPMG to do our financial statement audits, and part of that, we also do the I.T. part of it, we look at the FISCAM functions. There are five controls that we look at. We look at security management, access controls, integration management, segregation of duties, and contingency planning.

So as we go through not only CBP but various different components, we identified I.T. control weaknesses. Even though CBP has fixed some of those weaknesses in the previous year that we identified, there are still additional controls and weaknesses that we have found that they need to address.

So as, you know, part of the password protection and people being able to get into the systems, we have found not only in CBP but other parts of—even when we did within one of the components within NPPD we found almost a similar situation, so it is prominent throughout the Department.

So I think sending a guidance to the entire Department on best practices and, you know, one would think instead of having a password as "newuser1" one would change it as soon as they are able to log in, and then maintain that, as well. Not, you know, quite often you find people, you know, writing the username and password and leaving it under the keyboard and other places where people can find it.

So the—part of the review, what we did was we looked to, as the help desk we call up the component that we are doing the audit on and say, "I am from the help desk. Can you give me your username and password?" and without hesitation people tend to just give that up.

Ms. CLARKE. Mr. Chairman, I know that my time is lapsed here. I just wanted to add that, you know, we can put all of the new technologies we want in place but if cyber hygiene has not become a practice, the vulnerabilities remain perilous to us.

So I want to thank you for your report.

I yield back the balance—yield back to you, Mr. Chairman.

Mr. MEEHAN. I thank the gentlelady, and I share that same observation.

We are hearing—I know it is something you are talking about across the sector and we have heard testimony that more than 80 percent of our vulnerabilities could be addressed with better cyber hygiene. I think that is something—again, we talk about this process of educating America and the role that they can play with us. There is more sophisticated things and that is what you are dealing with, but we need the Nation to join us in battling the threat by doing better cyber hygiene.

Ms. CLARKE. We start with our own agencies, right?

Mr. MEEHAN. We start with our own agencies, that is right, by setting the example.

I am very grateful for that testimony, and now the Chairman recognizes the gentleman from Texas, Mr. Vela, for any questions he may have.

Mr. VELA. Yes. Yes. On the issue of workforce, can you begin by explaining to us how your different divisions interact?

Ms. STEMPFLEY. Thank you, sir.

In the Office of Cybersecurity and Communication we have five divisions, and those divisions span responsibility from National security emergency preparedness communications—that is the Office of Emergency Communications; the Office of Stakeholder Engagement and Critical Infrastructure Resilience, which is principally responsible for our outreach efforts, for our engagement with critical infrastructure to raise their understanding at a macro level, which is obviously supportive of the operational role that the NCCIC plays; as well as our Network Security Deployment Division, which is responsible primarily for the building and deployment of the—and operation of the National Cybersecurity Protection System; and finally, our Federal Network Resilience Division, which is focused on the dot-gov protections. That is both in terms of direct interaction with Federal departments and agencies and the building of the capability that you discussed earlier, the continuous diagnostics and mitigation capability, which is focused on the cyber hygiene for the Federal enterprise.

Those five divisions operate together under the Office of Cybersecurity and Communications. You can see the mutually supportive role that they pay.

For example, the communications infrastructure is moving to being I.P.-based. With an I.P.-based communications infrastructure you bring with it particular risks and opportunities. The technology awareness mechanisms of that are shared, then with the Stakeholder Engagement Organization and the threat information provided from the NCCIC is then disseminated and distributed.

That data all support the requirements that go into the National Security—excuse me, the Network Security Deployment Division, and the Federal—and we want the Federal Government to be the best example of the right things to do within the Federal Network Resilience Organization. We realigned this structure last November, so not quite a year ago. It has been a very beneficial activity for the Office of Cybersecurity and Communication.

Within the Department, the deputy secretary chairs a panel that ensures that we are—excuse me—coordinating across the Department. There is both operational engagement on the NCCIC floor from our Department colleagues for Secret Service, from Coast Guard, and others. We have policy conversations across the Department to ensure that we are sharing. We have a strong partnership with the CIO so that those FISMA requirements that we—the operational requirements that we publish in partnership with OMB are coordinated with and shared with the CIO organization to understand what that might mean to a large department that is informing back to us.

Mr. VELA. The Ranking Member mentioned—or referenced a problem with retention of workforce, and are you seeing that in each of those five divisions, or—can you explain that?

Ms. STEMPFLEY. Absolutely. It is a competitive landscape for cybersecurity professionals. We are actively recruiting.

If you look at the growth in terms of civilians that we have had in the Office of Cybersecurity and Communications in the 3 years I have been here, we have been actively engaged in this recruiting process. Mr. Zelvin shared earlier today with me a fact that, you know, for each announcement that we put out there we get candidates applying in numbers close to 100.

The issues that we have in this competitive landscape are that the Department of Homeland Security's authorities for meeting the hiring needs are not commensurate with the other Federal departments' authorities, and so both in terms of pay and retention capabilities, we are competing against our own colleagues in the Federal Government and continue to compete against our colleagues in the broad commercial landscape, as well.

We have a phenomenal mission and we keep people in part based on the mission responsibilities that we have. We do not have an exorbitant attrition rate at the operational level, certainly. People leave; they leave on, you know, based on their family and life desires. We don't see this, you know, exceptional attrition rate.

But we do see that strong competition.

Mr. VELA. So are you saying that you can't pay people enough, essentially?

Ms. STEMPFLEY. That is part of the issues, yes, sir.

Mr. VELA. I noticed that your title is you are an acting assistant secretary. At the levels of leadership are there many spots that have not been permanently filled?

Ms. STEMPFLEY. Within the Office of Cybersecurity and Communication the acting assistant secretary is the only leadership position that has not been filled—or the assistant secretary. I have full-time career leadership. I am permanently the deputy assistant secretary so I am the full-time careerist in that position. At each of the division director level I have full-time fill in, you know, all of those as career positions.

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

We now recognize the gentleman from Nevada, Mr. Horsford, for his questions.

Mr. HORSFORD. Thank you, Mr. Chairman.

Appreciate very much this panel. You know, we have been meeting, as one of the new Members on this committee, a lot of the peo-

ple in the private sector, and I want to commend the Center on its collaboration with a number of key private-sector entities and sectors.

My question pertains to this collaboration with the private sector.

You mentioned in your testimony the work with the over 6,400 private-sector firms that work with the Center, and inevitably some of those have to be competitors, of course. So can you discuss the protocols and measures that you all have in place to ensure that one company's sensitive data does not pass on to another, particularly to a competitor, and what procedures are in place should such an incident occur?

Mr. ZELVIN. Yes. Thank you, Congressman.

Last year alone, as Ms. Stempfley said, we had 190,000 incidents reported and we put out almost 8,000 reports. This year we are going to exceed that just in—by May about 68 percent.

So when we get information there is a variety of ways a business can report. They can tell us that it is okay to say it is their company, and that is not an often occasion; they can ask us to anonymize, and we have this thing called traffic light protocol, and it is literally just an agreement between friends that we will not share. When I first saw it I was somewhat skeptical but it actually works, and we have a variety of ways of quantifying using a stop light protocol—red, yellow, green, so on and so forth, and it is actually an effective means.

We have statutory capabilities under PII, Protected Infrastructure Information—I think I have the acronym right. But there is a statutory basis that we can anonymize information, and let's say, you know, you work for a financial sector. I will just refer to you as "financial sector seven," or "FIN7," or "FIN8." What is important is not the identity of the company but the ability to port across cross-sector what is happening and, more importantly, what do you do about it.

So we have folks on the floor at the NCCIC, so we have NSA, we have FBI, we have Secret Service, we have Cybercom. We also have all the information sharing and analysis centers of the financial services, communications, information technology, and also folks from individual companies that have full access to the floor even when we are at Top Secret or above classification. They have full access to all our computer systems, both the highly classified all the way down to below.

So as you have these folks on board we are very cognizant of the competitor aspect, so we have abilities to put a label that anonymizes it that is either done through agreement or through statutory. In the agreement, why do—you know, why wouldn't we share? Well No. 1, I don't really need the information; the second thing is I don't want to betray your trust because if I do you will never talk to me again.

So, you know, we are very cognizant of it and we are very successful at it, as well.

Mr. HORSFORD. So my other part of my question is, it seems like some sectors are better at this than others, so how concentrated are certain sectors in working with the centers and do you see gaps? If so, what can we as Congress do to help facilitate bringing

the sectors who aren't doing their part, you know, into the resources that you all have available?

Mr. ZELVIN. Yes, sir. Who has really focused on meeting the challenges really depends on their experience, as I mentioned, in cybersecurity and the attacks. There are certain sectors that have had a large number of attacks; there are others that haven't yet. It is all of our challenge to go out to them and say, "Hey, this is really what others are facing, these are the things that you could be facing, and these——"

Mr. HORSFORD. If I could be more specific——

Mr. ZELVIN. Sir.

Mr. HORSFORD. So these people come into my office every day and my job is to, you know, encourage them to participate. You all have great capacity among Federal agencies, but as I have heard it, as the Chairman and the Ranking Member have educated us, the vulnerability is on the private-sector side and the private sector isn't always doing its part, and there are key sectors that seem to be completely kind of disengaged. So what do you need from us as Congress specifically to get those sectors to be more involved?

Mr. ZELVIN. In my view it is the continued dialogue and the continued conversation that we are having. I think, as I look—you know, as I have briefed senior leaders, as I have briefed staff, you know, people generally understand there is a problem but they don't understand what to do about it, and when you talk about the problem they don't really—they know there is something wrong but they really have trouble quantifying what is it.

The other thing I will tell you—and I say this often—the lexicon in cyber is not English, so if I say "phishing," if I say "D–DOS," if I say "Trojan"—when I say "phishing" most people go to a lake someplace and think about, you know, maybe catching a fish but that is not when I am speaking of.

I have often said also is that if I told you there was a Category 4 hurricane that hit the Gulf Coast you would go, "Oh, that is bad." Category 1? It is bad, but 4 is worse.

If I told you there was an 8.0 earthquake on the West Coast you would automatically go, "That is incredibly bad." 1.0? Most Californians probably wouldn't do anything.

What is that in cyber? How do we get that imagery? How do we get the awareness across to the public of, "Boy, this is something that is bad but we could probably be okay," or, "This is catastrophic and we need you to do these measures such as leave, you know, other precautions."

So we are still working that and I am hopeful, but we are not there yet.

Mr. HORSFORD. Thank you, Mr. Chairman.

Mr. MEEHAN. I thank the gentleman. I certainly, you know, one of the aspects are the ISACs and other things that can be present, and I think the gentleman's questioning was right on target about those that are engaged and those we have to do a better job of attracting.

It is important to appreciate the vital role that you play and the interplay among our Governmental agencies at the outset before we get down to dealing with the various private-sector industries that are part of it, so I want to ask you to go for a moment off of

this important observations, and it comes from General Alexander, who is the head of the NSA, and I use it in his words, and he says, "I see the Department of Homeland Security as the entry point for working with industry," and there is great reasons for it: Transparency, having everybody doing exactly the right thing together to work as a team.

The FBI, NSA, Cyber Command—the FBI would lead law enforcement and the attributions; NSA will work with foreign intelligence; Cyber Command are defending the Nation. But they have a civilian agency, by his own testimony, at the core of the ability for us to have a communications infrastructure that works across the Governmental sectors first and then simultaneously work effectively in real time with our civilian sectors.

So please give me your observations with regards to somebody as significant as General Alexander looking at DHS as the center point for the engagement of our approach to cybersecurity.

Mr. ZELVIN. Thank you, Mr. Chairman.

I agree with the general's assessment so much so I joined the Department. DHS is purely that civilian entity, and when folks come to us they know—and there is important other roles in Government, but within DHS we are really about that protection, prevention, mitigation, response, and recovery. We really do want to help understand the problem not only technically but through the tactics, techniques, and procedures, and then work through those mitigations, and then share that information, as I said, with the partners I have mentioned—State, local, critical infrastructure, international, other Federal departments and agencies.

So when folks come to us—and it has been interesting. A number of private-sector partners have come to us because they see us as that place in Government where they can have a discussion where it is purely technical, there is not concerns potentially of being asked a lot more questions that will lead to other things and it is important for Government to do.

As you look at vulnerabilities in cyberspace, there are things that have the potential for malicious activity but haven't quite matured to that point yet, and I look at things like have happened to a number of companies in that we discover a vulnerability that if somebody did something it could be catastrophic, but they haven't done it yet. Those are really the areas that we want to get ahead of.

We don't always want to be responding. We don't always want to be catching up to our adversaries. We want to get ahead of those.

For companies it can be often uncomfortable to say, "We discovered a problem," and they don't want to be attributed—they don't want their competitors to say, "See, look. They are having yet another problem." So they come to us and we have the ability to provide the anonymity, work through the technical solutions, and then get it across the Nation and across the world so people can understand the threat and mitigate it without the fear of additional questions about who did it and where did they do it and how.

Mr. MEEHAN. Effectively, you are a civilian agency so it removes some of the concern that legitimately people have outside that we are having private sector share either back and forth with our more sophisticated Governmental agencies like the NSA or FBI.

Mr. ZELVIN. That is correct, sir. It is absolutely a civilian organization and I don't have the challenges that some of my partners do in that I am not being pushed for things like attribution; I am not being pushed for bringing prosecution. There are other important entities that do that; that is not my role. My role is just to understand the problem and come up with the solutions.

Mr. MEEHAN. Let me jump into one other piece, because we have done a good job of identifying the important role we place vis-á-vis the other Governmental—critical Governmental agencies, and of course, that extends down through the entire Governmental structure. But at the same time, we have relationships with the private sector.

Now, those looking from the outside can get lost in forest, but there has been a lot of thought into how we are organized and I am impressed by it. Explain quickly: We have 16 different sectors—17 different sectors in which industries are organized, and they have their own sector communication coordinating councils in which they themselves look at the unique nature of threats, such as something that may go uniquely to banks, the denial of services as an example.

Within those coordinating councils some—and this goes to Mr. Horsford's line of questioning—some have created what we call the ISAACs, these information sector analysis coordinating teams—very sophisticated for their—and they are housed with you. But my recollection is we have only got about four that are in there. They are some of the best, but we have got a lot of agencies or private-sector entities that may be lagging.

Can you give me your observations with regard to how it is that, you know, we are effectively organized in that way but what we can do to begin to attract the collaboration of all of the other entities?

Mr. ZELVIN. Yes, Mr. Chairman.

We deal with all of the critical infrastructures. We are working across the board. But I will tell you, as I look across the financial services sector, and specifically the Financial Services Information Sharing and Analysis Center, the FS–ISAC, they have done an absolutely extraordinary job helping us work through the recent distributed denial of services hacks that have been going against the financial institutions.

So the Financial Services ISAC has not only been able to coordinate with Government, but also among itself. They provide extraordinary information not only with each other but also with Government. Some of the best information I get from the distributed denial-of-services comes from the private sector, and it is not only the sharing with us but also sharing within each other.

The Communications ISAC, the Information Technology ISAC have similar experiences. I will also tell you, the Multi-State ISAC, so the sharing between all the States and the possessions and the territories—that information mechanism is very effective.

There are others that we need to build up to that capacity, but I would tell you, I don't see that as a negative; I see it as a positive. We have learned a lot since these distributed denial-of-services attacks, and also the malware attacks that have affected Saudis and also in Qatar.

This has changed the dynamic in cybersecurity just in the last few months. So ideas that were really well-thought-out earlier are really being developed and we need to catch back up with the others as we stay focused on the financial services sector, the comms, and——

Mr. MEEHAN. You mean you are learning things with financial services that could apply to other sectors.

Mr. ZELVIN. That is exactly right, sir. I often tell folks that we need to share this across because the financial services sector needs power, they need water, they need transportation, they need health. They say, "Why would we share with you? Why would you tell DHS?" Well, because we have the ability that is unique in that we can share with these other sectors and we can make them aware of the challenges and we can share the mitigations, so why would you rebuild that capacity when it already exists?

Mr. MEEHAN. Well, thank you.

My time is expired and I now recognize the gentlelady from New York for her follow-up questions.

Ms. CLARKE. Let me thank you, Mr. Chairman, and acknowledge that we have been joined by our colleague on the Homeland Security Committee, the gentlelady from Texas, Ms. Jackson Lee, and ask for unanimous consent that she be authorized to sit and question the witnesses at today's hearing.

Mr. MEEHAN. Pleased to do so. Unanimous consent, the gentlelady will be recognized in order, and I thank her for coming today.

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

I want to question each of you, just get your perspective on the dichotomy between the Enhanced Cybersecurity Services and Einstein. I support the expansion of the Enhanced Cybersecurity Services program to make sure that our critical infrastructure companies can benefit from U.S. Government intelligence on cyber threats. However, in the privacy impact assessment the Department states that Federal agencies as well as critical infrastructure may use ECS while the Einstein intrusion prevention capabilities are still being built out.

My question is: Doesn't it seem a bit backwards or redundant, and how is it that you could build a cutting-edge cybersecurity program and have it available to the private sector before the Government itself adopts it? What is it about ECS that will make it available much more quickly than Einstein 3?

Ms. STEMPFLEY. Thank you, ma'am.

The Enhanced Cybersecurity Services is, as you point out, a cutting-edge capability in that it is the first time we have been able to provide effectively classified and sensitive countermeasures and indicators to commercial entities through a trusted cybersecurity provider, I think is very important. So we are very excited about this opportunity and engagement in both growing the number of service providers and the market that it generates with critical infrastructure partners.

It provides, as you point out, in the privacy impact assessment, protection against—with two countermeasures: Domain name service and e-mail protection. Those are not in the traffic flow kinds of

protection, which is the requirement for Einstein 3, and so there is a fairly important distinction there.

While we will work to enhance the Enhanced Cybersecurity Services, enabling it to keep up with the threat environment and to provide new countermeasures into that capability, we are certainly in progress in that environment. We will reach that in a much more rapid manner in the Einstein 3 capability because its baseline requirement is to provide that in a real-time capability inflow.

That is a very technical way of describing—a technical way of describing it, the difference being inflow means you are actually affecting through the pipe as it is going on; out of line effectively means it gets stored, processed, and then forwarded on.

Mr. ZELVIN. Ma'am, I will tell you, there is some—I have a truly exciting job, and one of the really exciting parts is as you look at that dot-gov domain and the security awareness that I have, it is unlike any of others—so you have the dot-com, the dot-gov, and the dot-mil.

So right now on the dot-gov I have extraordinary awareness of the traffic that is going on and we are watching that in almost a real-time basis in my center at the NCCIC. I have met with the Defense Department and we are building an awareness of the dot-mil similar to what we have on the dot-gov. So between the two of us we will have really strong awareness of what is going on.

The dot-com will remain a challenge, but DHS has that dot-gov responsibility. We are able to watch it, as I said, on a near real-time basis, and as we get these new enhancements, what we are able to do now is just to be able to see there is malicious activity and warn. What we will able to be doing here shortly is just not warn but actually mitigate and investigate and analyze.

Because right now it is sort of like you know there is something bad in the mail but you let it get to the mailbox. Well, now we are going to be able to stop that and do appropriate measures to make sure that that bad delivery isn't made.

Mr. EDWARDS. I will just agree with both Larry and Bobbie on this.

Ms. CLARKE. Very well.

So is it anticipated that at some point the ECS will be phased out or become obsolete, or is there a unique capability within that instrument that is compatible or can partner with Einstein 3?

Ms. STEMPFLEY. Certainly. The ECS is intended to be a program for that information sharing and protection for the critical infrastructure. It has very, very limited report back to Government, obviously. Only, "Did that indicator work? Is that a valuable piece of information for protection measures?"

We would anticipate that to continue and that we would employ more countermeasures as we go through the legal, privacy, and other considerations for employment of those countermeasures in the unique situation of critical infrastructure.

E3, and E3 Accelerated in particular, and its wide set of capabilities for the Federal enterprise we anticipate existing, as well. The specific countermeasures and which one would come forward into the Government space or the critical infrastructure space is really based on the very different legal models that are appropriate for us in that space.

Mr. MEEHAN. I thank the Ranking Members.

The Chairman now recognizes the gentlelady, Ms. Jackson Lee, for any questions she may have.

Ms. JACKSON LEE. Let me thank, first of all, the Chairman and the Ranking Member for holding the hearing and your courtesies of allowing me to come and to ask questions for something that I think is crucial for the entire Homeland Security Committee.

Let me start out—and I am going to just offer for you to answer the questions who can answer it, and I will then ask the particular person if no one jumps in. The CERT teams that we have—this is enormously important, this whole idea of communication, the whole idea of reacting to the cyber threat—with respect to the CERT systems, do we have the capacity to have a particularly defined CERT for each of the industries? I think of oil and gas; I think of the health-care industry, which is massive.

That is my first question: Do we—are they defined so specifically that they focus on the needs of a particular industry?

Madam Secretary.

Ms. STEMPFLEY. Ma'am, if I may take a——

Ms. JACKSON LEE. Yes. Thank you.

Ms. STEMPFLEY [continuing]. A first crack at your question, the technologies that are in use across these industries are very similar, and because of that the organization of our cyber emergency response teams or computer emergency readiness teams are oriented to be useful to all of the sectors, versus a particular emergency readiness team focused on any one sector. So you see the information technology infrastructure largely covered by the US–CERT, then the operational technology control systems community operated by the Industrial Control Systems CERT.

So the infrastructures in the oil and natural gas, or in transportation, or in those mechanisms are largely produced by the same companies and in the same environment. This has proven to be one of the most effective and efficient organization models.

Ms. JACKSON LEE. Let me follow it with two questions, and maybe I will have time to make a comment. Thank you for that.

We all understand that finding a problem in computer security or cybersecurity is like finding a needle in a haystack, and so have we developed the sophistication to be able to target where the problem is, to target where there is activity?

My other question is on the Einstein 3 I notice that there is certainly a need for skilled individuals, and my question is: Do we as the Government have the capacity to bring people in laterally? It speaks to my issue of the STEM and diversifying. STEM education is great but it starts at kindergarten. If we need people right now, do we have the ability to cross-train them in the Government, which adds to the diversity and the skills that we need?

I will—those are the two questions I will pose.

Mr. ZELVIN. Congresswoman, if I can maybe finish your first question and get to the second and——

Ms. JACKSON LEE. Yes.

Mr. ZELVIN [continuing]. Ask Ms. Stempfley to do the third. So on the first question on the specific CERTs for each of the sectors, I will tell you that when we operate in a sector we do it in intimate partnership with the sector-specific agency and the sector-specific

coordination councils. So if there is an energy problem we are with the Department of Energy; if it is oil and natural gas, Department of TSA; Finance; Treasury; so on and so forth. We are fully partnered.

So we bring the technical skills, the ability to understand the virtual and I.T. environment. They bring the experience and wealth of knowledge within——

Ms. JACKSON LEE. Do we have the capacity to target if there is activity that is in essence piercing our cyber framework involving our proprietary information? If somebody is attacking our system, you have that capacity?

Mr. ZELVIN. We have the—some capacity. We do not have absolute capacity.

Ms. JACKSON LEE. What would you need to get absolute capacity?

Mr. ZELVIN. Extraordinary intelligence and information. So, you know, in many cases there is vulnerability. So there was a mistake made and then found, and so there are things you do to correct that mistake.

There are attacks. There are people who are purposely trying to do something you do not wish them to do. In many cases and not all—in many cases you are there reacting to the challenge and then building that technical mitigation to prevent.

However, there are times they are are going to be—you know, we have to be good every time; they have to be good just some of the time. So I would never say that we are ever going to get to that place where we will be able to protect everything, but we have a great deal of information but it doesn't mean that we don't have vulnerabilities.

I would ask Ms. Stempfley to follow up.

Ms. STEMPFLEY. We want to certainly thank Members of this committee and others for supporting the resource request that the Department has had over a number of years. You have seen the build-out of the capabilities in the National Cybersecurity and Communications Integration Center, which has been directly to your capacity question. We operate every day in that center, sharing information as a part of it.

There is a responsibility the private sector has for adoption of best practices and adoption of cybersecurity principles, and we continue to work with them for further movement in that area.

Your final question was on hiring and, in particular, is there—if I understood your question correctly——

Ms. JACKSON LEE. Cross-training.

Ms. STEMPFLEY. Right. So is there an ability for lateral hiring, I believe is what you said. One of the things that I think is universally recognized is that, given the importance of cybersecurity and the need for cybersecurity professionals in this area, we—all of the Federal enterprise and our commercial partners are engaged in trying to build the capabilities to ensure we have that.

The Secretary chartered, through the Homeland Security Advisory Council, a cyber skills study that looked at the Department itself. The Department also has important responsibilities under the National Initiative for Cybersecurity Education, which continue to engage raising that lateral mechanism, that cross-skills.

We certainly have to focus not only on, as you point out, STEM starting young—I am raising several kids who I am trying to direct into the technical workforce, as well—but to ensure that we have the capacity at a lateral level.

We do this cross-training support in the Office of Cybersecurity and Communications. When we have an incident the NCCIC can call on individuals from across the SNC, can call on individuals from across the Department. One of the findings out of the Cyber Skills Task Force was the creation of a cyber surge capacity within the Federal Government and the Department specifically, to address your question.

Ms. JACKSON LEE. I would like to follow up with you.

I thank the Chairman and Ranking Member for their courtesies. Thank you very much.

Mr. MEEHAN. I thank the gentlelady for her attendance here and for her questions.

I just have one—a couple of closing questions based on your testimony here today.

Mr. Edwards, you identified something which goes to the reality that while we are dealing with a lot of these issues and the need for collaboration across sectors in the Government and, simultaneously, with the private sector, one thing you focused on that is the reality of this threat is speed. It is happening in real time and there is a need for us to be responsive in real time.

Now, you have looked critically at the challenges that we face, so the first issue is, as you stated, sometimes information has gotten to our partners in the private sector but we have got to do a better job of organizing it so it allows them to get to the heart of what they need to know. The second thing is that we have got to try to find ways to be able to coordinate with our partners more in the sense of: "Hey, we are seeing something in your systems and we are going onto it."

So how do we both maximize our ability to get the information that people need to know across sectors, not just in sectors? Then how do you tell people—when you are not even sure what you are looking yourself, where do you find the right balance of telling somebody you might be looking at something in their systems versus creating an alarm that may not be realized because you don't know what you have yet?

Mr. EDWARDS. Thank you, sir.

The Department has done a good job in advancing cybersecurity. One of the recommendations that we made was when you are passing out this information through—whether it is HISN, and now they are going to move to HISN–3—is to—for the entities to be able to share that information, you know, and also not to drill down to get to a particular question they are trying to answer. So I think HISN–3 is going to help towards that.

But also the communication part of it. You know, there is excellent collaboration between the private sectors and the public sectors.

But among the folks that we interviewed, quite often we found is a lot of this is also based on relationships, and the Department has senior leadership positions where people from the private sector pick up the phone and establish a relationship to somebody by

name and now that person has moved on, they don't know who to contact. So rather than establishing relationship based on individuals, it needs to be based on processes and procedures, and I think the Department is moving towards that.

But also, there is—private sector does a really good job in handling best practices. Larry's team, you know, by the reorganization and putting ICS and US–CERT and ISAC and C3O–I, all of them at one level is moving toward that. But you also find information and trend analysis that the CERT team is going to help towards that.

Mr. MEEHAN. Well, I thank you.

Let me just ask Mr. Zelvin and Ms. Stempfley, how about the private-sector companies themselves sharing information with the Government? What kinds of challenges do we have in that area?

Mr. ZELVIN. Thank you, Mr. Chairman.

The biggest challenge, I will tell you, is a lack of clarity, of understanding what information can be shared. So it is quite often that we will meet with private sector entities and we are—we believe we have the ability to share information but there is anxiety. There is absolute determination not to violate law, regulatory guidance.

Mr. MEEHAN. Is this information coming from you to them or from them to you?

Mr. ZELVIN. From them to me, sir. There is also, you know, lack of clarity as to what I can share with them but, you know, as we have looked across Government I have been given the thumbs-up from leadership and also those who look at what we are sharing in—across Government and says, "No, this is appropriate and this is okay."

But that lack of clarity of what information can be shared is—still exists and there is anxiety, so——

Mr. MEEHAN. What is the anxiety related to? Things like liability protection or otherwise?

Mr. ZELVIN. It is, sir. The ability to, as I said, that they are not breaking law, that they are not breaking regulatory compliance. They are just not sure so they err on the side of caution.

As you mentioned, Mr. Chairman, speed is of the essence, so as the folks review all this data it is taking up precious time. We have, in our—many of our products and what we are starting to receive from the private sector and just recently this week an international partner is machine-readable information. That is wonderful because it is starting to take the humans out of the information exchange between us. What would be even better someday would be that machine-to-machine real-time information sharing.

But I will tell you, the technical challenge is not, in my opinion, as great as the policy challenge. We first have to define what is it that we are sharing, and then we can design the machines to share it.

Mr. MEEHAN. Well, with the tremendous scope of information, ultimately it is going to have to get to machine-to-machine because of the computing capacity that could go through something in hundredths of a second that would take days for humans to be able to analyze.

Mr. ZELVIN. Mr. Chairman, I agree. Right now there is a great deal of time spent preparing the information, sending the information, understanding the information, and then making the information actionable. We need to compress that loop of decision-making as small as we can get. I don't know if we will ever get to zero but we sure as heck can do a lot better than we are now.

Mr. MEEHAN. Okay.

Ms. Stempfley.

Ms. STEMPFLEY. Sir, one of the important things that the I.G. recognized and Mr. Zelvin spoke to is that this information sharing is in part based on trust, and you have to have a sense that the information will be used in the best interest of all parties as we go forward. That trust used to be person-to-person. We have moved it from person-to-person to organization-to-organization and we will continue to do so.

One of the important ways that we are moving forward in this model is to communicate with our private-sector partners in ways that are most beneficial to them, which means that we have to be able and willing to ingest that information in the method that is most appropriate from our private-sector partner, and we must be able to produce our indicators, our alerts in methods that are appropriate without a—with a recognition that it may not be identical. We talk about the financial sector and the financial sector ISAC being one of our mature ISACs, and there being other sectors who are not at that level yet.

So providing a piece of information to a high, capable organization may prove for it to be not as useful to an organization that isn't ready to ingest that. So we have had a real focus, not only in the NCCIC but across the entire Office of Cybersecurity and Communications, to release this information in a multitude of platforms and in a multitude of formats. So this machine-consumable output is formatted in a way that can be consumed by these different entities.

This two-way dialogue helps to build that trust, which is a part of what we have to overcome is that sort of initial distrust that comes in any relationship.

Mr. MEEHAN. Well, I thank you for the good work that each of you is doing, and on behalf of all of your entities, for not only creating the framework for this sharing of communication but by virtue of the collaboration that you are doing, enhancing that trust and enhancing our ability to protect our home front from the serious threat. We opened this hearing with discussing the very real concern about cybersecurity here in the Nation.

Is there any closing thought that you—any of you have before we close the record this morning?

Ms. STEMPFLEY. If I may, I want to thank you again for this hearing. I think it is—the topic is one of absolute import for us as a Nation and we are grateful for your attention and your time here.

I hope that you heard the commitment the Department has to this important mission and to ensure that we account for those mechanisms that are so vital: That inextricable tie between privacy, civil rights and civil liberties, and cybersecurity; the need for adoption of security principles across our critical infrastructure partners for information sharing.

We talked about some of the important needs for hiring authorities for some of the programs that I know you are supportive of in Einstein. Our law enforcement colleagues in the Department continue to seek tools they need to fight crimes in the digital age, and that National breach reporting requirements that I know you are discussing.

So thank you so much for your time and attention on this matter, as well.

Mr. MEEHAN. Thank you.

Mr. ZELVIN. Mr. Chairman and Ranking Member, I would just also like to thank you for having us today. Really appreciate the opportunity to talk to you.

You, your colleagues, your staff, and their colleagues are welcome at the NCCIC any time. We would welcome the opportunity to show you what the great men and women within the NCCIC, within CC&C and DHS are doing.

I served 26 years in uniform in the Defense Department and I will tell you, the people that I work with at DHS every day are as good as fine as anyone I served with in uniform. Their passion and their patriotism are just as high as those I served with in uniform.

I would also like to say that our partnership with our closest colleagues, both in the FBI and NSA, is critical. So it is truly a unity-of-effort approach, and that integration continues to grow and we look forward to the opportunity of having it grow not only within Government but also private sector and international.

So thank you.

Mr. MEEHAN. Thank you.

Mr. Edwards.

Mr. EDWARDS. Well, we live in a virtual world so, you know, DHS has matured and it is improving and it is moving in the right direction, but much work still needs to be done. The threat is not only going to be coming from nation states, but from hackers, but also the threat within. We have to be mindful of that.

I hope I can come back and issue a report and say the Department has done perfectly everything right and there are no findings and no recommendations. That is what I hope I can do, but still there is much work to be done.

Thank you.

Mr. MEEHAN. Well, we would all love to be able to do that, but that is the important responsibility we have on oversight and we thank you for the good work that you are all doing to try to aspire to that standard.

So I thank all of you for your testimony. The Members of the committee may have additional questions, and if they do we will ask you to respond in writing in the appropriate time.

So without objection, the subcommittee stands adjourned. Thank you.

[Whereupon, at 10:32 a.m., the subcommittee was adjourned.]