STRIKING THE RIGHT BALANCE: PROTECTING OUR NATION'S CRITICAL INFRASTRUCTURE FROM CYBER ATTACK AND ENSURING PRIVACY AND CIVIL LIBERTIES

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

APRIL 25, 2013

Serial No. 113–13

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

82–587 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

STRIKING THE RIGHT BALANCE: PROTECTING OUR NATION'S CRITICAL INFRASTRUCTURE FROM CYBER ATTACK AND ENSURING PRIVACY AND CIVIL LIBERTIES

Thursday, April 25, 2013

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

The subcommittee met, pursuant to call, at 2:19 p.m., in Room 311, Cannon House Office Building, Hon. Patrick Meehan [Chairman of the subcommittee] presiding.

Present: Representatives Meehan, Rogers, Daines, Perry, Clarke, Keating, Vela, and Horsford.

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 balance between preventing a cyber attack on our Nation's critical infrastructure and ensuring privacy and civil liberties are protected. I will recognize myself for an opening statement.

I would like to welcome everyone to today's hearing, which is titled, "Striking the Right Balance: Protecting Our Nation's Critical Infrastructure From Cyber Attack and Ensuring Privacy and Civil Liberties." During this Congress, our subcommittee has been examining the cybersecurity threat to individuals and to our critical infrastructure. Our Nation has made great strides, but the threat is multi-faceted and we are only as strong as our weakest link.

Earlier this week, we saw the ramifications of a hacked Twitter account that nearly sent our financial markets into a tailspin. While the Dow Jones Industrial Average has to recoup their losses, the lesson is clear: We are in an interconnected world. A successful attack on one network will certainly impact others.

The Department of Homeland Security plays a crucial role in preventing cyber attacks on our Governmental and critical infrastructure key resources. As Chairman McCaul and I and the Ranking leadership work together, we have continued to use our efforts to craft legislation to bolster existing structures and improve the capabilities of the Department of Homeland Security. One of the key challenges will be to strike the balance of securing our networks and ensuring our protections for our citizens.

Upon assuming the gavel of this subcommittee this year, I made sure I immediately reached out to leading privacy advocates. Groups like the American Civil Liberties Union and Center for Democracy & Technology have been instrumental in shaping the thinking as we have moved forward with the committee's work. Indeed, we must make clear that the purpose of sharing information is to prevent a cyber attack and nothing else. Any intelligence shared with the Government or with public or private entities must include protections for consumers and individuals.

In order to accomplish this, we must ensure that we have a full understanding, first, what the threat is; next, what type of intelligence is necessary to share to prevent an attack; then what type of information is inadvertently caught in the net; and furthermore, what may be done once it is identified? The answer to these questions, coupled with robust civilian oversight, a clear set of rules of conduct and liability protections for those acting in good faith will help shape the key policy initiatives for our subcommittee.

I need to be clear and I think all of us share that right out front that the committee is not concerned with internet habits of ordinary Americans. It is our duty as Members of this committee to make sure that the Department does not monitor, collect, or store the on-line activity of law-abiding American citizens. Therefore, information that permits the identity of an individual to be directly or indirectly inferred, which is also referred to as personally identifiable information, must be protected.

The Department of Homeland Security has significant inherent advantages that enable the Department to facilitate communication among 16 critical infrastructure sectors. The Department of Homeland Security Privacy Office is the first statutorily required privacy office in any Federal agency. The office is responsible for evaluating Department operations for potential privacy impacts and providing mitigation strategies to reduce the privacy impact.

By employing Fair Information Practice Principles, or FIPPs, as it is known, the DHS Privacy Office is charged with ensuring that the Department's data collection methods are transparent, have specified purposes, and include data minimization, use limitation, data quality and integrity, security, accountability, and auditing. Those are FIPPs principles.

It is for these reasons that many intelligence and cybersecurity experts point to DHS as manning a significant role in combating the threat. In fact, the Director of the National Security Agency, General Keith Alexander, said that due to the Department's transparency, he sees DHS as an entry point for working with industry.

Building our Nation's capacity to prevent cyber attacks is complex as it is essential. As a former United States attorney, I can tell you that the Department of Justice has a very important role to play in enforcing our cyber crime laws. We also must permit our military and foreign intelligence capabilities and those resources to protect our Nation's defense. Equally as important, the Department of Homeland Security has the mission of defending our Nation's key resources and the liberties guaranteed by our Constitution.

We have an excellent panel of witnesses today who will help us answer these questions and hopefully help us find the balance. Moving forward, today's hearing aims to examine how DHS cur-

rently protects privacy and personally identifiable information. It addresses the legitimate privacy concerns that are inherent in sharing cybersecurity threat information and finds ways to strike that proper balance between privacy and security. No one should mistake the common cause of securing our homeland for authority to violate the civil liberties of Americans.

The Chairman now recognizes the Ranking Minority Member, the gentlelady from New York, Ms. Clarke, for any statement she may have.

Ms. CLARKE. Mr. Chairman, I thank you for holding today's hearing. I am pleased to be joined today by this very distinguished panel of witnesses, and I would like to welcome Mary Ellen Callahan back to the committee for her first time since leaving the Department.

Here on the Homeland Security committee, we have understood the need to balance security and privacy for quite some time. Protecting our Nation from 21st Century threats requires vigorous coordinated action from our Government and State, local, private sector, and international partners. But if we go overboard to identify and eliminate every conceivable threat at any cost, we risk trampling the very rights of citizens we aim to protect. The need to find that proper balance has been a cornerstone of our committee's work on counterterrorism, on transportation security and certainly on today's topic, cybersecurity.

Most of the Government's efforts in cybersecurity do not directly touch upon privacy issues, and that is an important distinction that is not made often enough. Many programs, such as the Department of Homeland Security's EINSTEIN program, do not involve the collection or sharing of any kind of personally identifiable information at all. The vast majority of all of the information needed to thwart cyber attacks consists of technical data, such as IP addresses and malicious code, which has little or nothing to do with someone's social security number or passwords.

But where the private sector needs to share information with the Government to stop cyber attacks, every precaution must be taken to ensure the privacy of our citizens is ensured.

Last month, we heard from the American Civil Liberties Union on the importance of protecting privacy in cyberspace. I am pleased that we are joined today by three witnesses, who can really speak to the nuts and bolts of challenges, protecting private data from both the Government and business perspectives. As we look toward crafting our own legislation to help protect critical infrastructure and improve our Nation's cybersecurity efforts, it is important to really nail down the specifics of protecting privacy.

In order to get our approach to cybersecurity and privacy right, we must examine it from all the angles. We must assess the current legal environment and identify challenges that companies must cope with in ensuring the privacy and security of their employees' and customers' data. We must determine the types of information needed by the Government to prevent the attacks and the intended uses of that information. We must examine how commercial cybersecurity providers interact with their customers and the Government to share threat information.

Thankfully, our witnesses today cover the breadth of these issues with their testimony.

I am particularly pleased we are joined by Harriet Pearson, who is one of the Fortune 1,000 first chief privacy officers and has been a trailblazer for developing information policies and practices for protecting the private data of employees—excuse me, consumers.

Every American values their privacy and civil liberties as well as their security in cyberspace. I am confident that in building a lasting solution to our cybersecurity, we can adopt measures that will satisfy privacy advocates, the business community, and our citizens.

That ends my statement, Mr. Chairman, and I yield back the balance of my time.

[The statement of Ranking Member Clarke follows:]

STATEMENT OF RANKING MEMBER YVETTE D. CLARKE

APRIL 25, 2013

Here on the Homeland Security Committee, we have understood the need to balance security and privacy for a long time. Protecting our Nation from 21st Century threats requires vigorous, coordinated action from our Government and State, local, private-sector, and international partners.

But if we go overboard to identify and eliminate every conceivable threat at any cost, we risk trampling the very rights of the citizens we aim to protect. The need to find that proper balance has been a cornerstone of our committee's work, on counterterrorism, on transportation security, and certainly on today's topic, cybersecurity.

Most of the Government's efforts in cybersecurity do not directly touch upon privacy issues, and that is an important distinction that is not made often enough. Many programs, such as the Department of Homeland Security's EINSTEIN program, do not involve the collection or sharing of any kind of personally identifiable information at all.

And the vast majority of the information needed to thwart cyber attacks consists of technical data such as IP addresses and malicious code, which has little or nothing to do with someone's social security number or passwords. But where the private sector needs to share information with the Government to stop cyber attacks, every precaution must be taken to ensure that the privacy of our citizens is ensured.

Last month we heard from the American Civil Liberties Union on the importance of protecting privacy in cyberspace, and I am pleased that we are joined today by three witnesses who can really speak to the nuts-and-bolts challenges of protecting private data, both from the Governmental and business perspectives.

As we look towards crafting our own legislation to help protect critical infrastructure and improve our Nation's cybersecurity efforts, it is important to really nail down the specifics on protecting privacy.

In order to get our approach to cybersecurity and privacy right, we must examine it from all the angles:

- We must assess the current legal environment and identify challenges that companies must cope with in ensuring the privacy and security of their employees and customers' data;
- We must determine the types of information needed by the Government to prevent attacks, and the intended uses for that information;
- And we must examine how commercial cybersecurity providers interact with their customers and the Government to share threat information.

Thankfully, our witnesses today cover the breadth of these issues with their testimony. I am particularly pleased that we are joined by Harriet Pearson, who was one of the Fortune 1000's first chief privacy officers, and has been a trailblazer for developing information policies and practices for protecting the private data of employees and consumers.

Every American values their privacy and civil liberties as well as their security in cyberspace, and I am confident that in building a lasting solution to our cyber insecurity, we can adopt measures that will satisfy privacy advocates, the business community, and our citizens.

Mr. MEEHAN. I thank you, Ranking Member.

The other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

APRIL 24, 2013

We are here to discuss ways to secure cyberspace and critical infrastructure from hackers while assuring that Constitutionally-guaranteed privacy and civil liberties are safeguarded.

In the last 10 years, our society has become increasingly connected by computer networks. Networking technologies have changed our traditional notions of time and space. Our ability to reach the farthest corner of the earth has grown while the distance between us has shrunk. The world and all it has to offer is a click away and can be viewed on a screen in front of us.

But this unprecedented connectivity and convenience has not come without a price. We face new kinds of dangers that may come for us at any time from any corner of the globe. Destruction can be delivered with a keystroke.

Unfortunately, cyber attacks are increasing. This Nation cannot unnecessarily delay implementation of cybersecurity programs to combat these threats. Those efforts must include responsible collaboration between private industry and the Government to ensure the greatest care is given to our citizens' private data. The protections we put in place and the information we share to combat the threats must not undermine the privacy that each American rightfully regards as a fundamental freedom.

Working together, we can create a legal framework which encourages businesses to share enough information to reduce the likelihood of intrusions and prevent future harm without compromising privacy.

But, Mr. Chairman, perhaps the most important weapon in our arsenal to protect privacy is ensuring that the Government's efforts are led by a civilian agency. Information sharing with Federal civilian agencies will provide the public with a sense of increased transparency and accountability because Congressional oversight and public information requests will enable Members of this body and members of the public to peek behind the curtain, ask questions, and find out what is happening.

That is why I was proud to sponsor, with Chairman McCaul, an amendment to the Cyber Intelligence Sharing and Protection Act, which firmly established a center at the Department of Homeland Security to serve as the hub for cyber threat information sharing. As you know, this amendment was approved.

Mr. Chairman, I thank you for holding today's hearing to bring the privacy question into sharp focus. In the coming months, I look forward to introducing legislation to further improve our Nation's cybersecurity posture, with a special emphasis on privacy implications. I would like to thank our witnesses for joining us today. I look forward to hearing the testimony.

Mr. MEEHAN. We really are pleased to have a very distinguished panel of witnesses before us today on this important topic. I don't think that there could have been a better group assigned, but this is a remarkably important issue, and I think you have the ability to help the American citizens understand where this area is in which important work is done to allow us to protect our homeland, but simultaneously significant and important work is being done and can be done to help us ensure that we protect the privacy interests of Americans. So I am hoping that we can educate those who don't really understand in this complex area what the parameters are.

We have in this panel Ms. Mary Ellen Callahan, who we have had the privilege of having before this committee before, a Nationally recognized privacy attorney with an extensive background in consumer protection law. As the longest-serving former chief privacy officer of the United States Department of Homeland Security, the first statutorily-mandated privacy officer in any Federal agency, Ms. Callahan has a unique and broad knowledge of experience

with the interface of protection of privacy, civil rights, and civil liberties with cybersecurity and National security issues.

During her tenure at the Department of Homeland Security, Ms. Callahan also served as the chief Freedom of Information Officer, responsible for centralizing both FOIA and Privacy Act operations to provide policy and programmatic oversight and support implementation across the Department.

Ms. Callahan is a founder and chair of Jenner & Block's privacy information governance practice.

We have Ms. Cheri McGuire, who serves as vice president for global government affairs and cybersecurity policy at Symantec, where she is responsible for managing a global team focused on cybersecurity, data integrity, and privacy issues. Prior to joining Symantec, Ms. McGuire served as the director of critical infrastructure in cybersecurity in Microsoft's Trustworthy Computing Group and also as Microsoft's representative to the Industry Executive Subcommittee on the President's National Security Telecommunications Advisory Committee. Prior to joining Microsoft Ms. McGuire served in numerous capacities at DHS including as acting director and deputy director of the National Cybersecurity Division and US–CERT.

We are very pleased to be joined as well by Ms. Harriet Pearson, a partner at Hogan Lovells, where she focuses on counseling clients on privacy and information security policy in compliance matters, data security incident response and remediation and information in cybersecurity risk management and governance. Ms. Pearson joined Hogan from IBM Corporation where she served as vice president, security counsel, and chief privacy officer. At IBM, she was responsible for information policy and practices affecting over 400,000 employees and thousands of clients. She also lead IBM's global engagement public policy and industry initiatives relative to cybersecurity and data privacy. I think that outlines the tremendous qualifications and experience of this very, very distinguished panel.

So the witnesses' full statements will appear in the record.

The Chairman now recognizes Ms. Callahan for her testimony.

STATEMENT OF MARY ELLEN CALLAHAN, PARTNER, JENNER & BLOCK, AND FORMER CHIEF PRIVACY OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. CALLAHAN. Thank you very much, sir.

Chairman Meehan, Ranking Member Clarke, distinguished Members of the subcommittee, thank you for the opportunity to appear before you again today.

My name is Mary Ellen Callahan, and I am a partner at the law firm of Jenner & Block, where I chair the privacy and information governance practice and counsel private-sector clients on integrating privacy and cybersecurity.

As the Chairman noted, from March 2009 to August 2012, I served as the chief privacy officer at the U.S. Department of Homeland Security. I have worked as a privacy professional for 15 years and have National and international experience in integrating privacy into business and Government operations. I am appearing before this subcommittee in my personal capacity.

As the subcommittee knows and as Ms. McGuire will detail more thoroughly, the United States critical infrastructure faces significant cybersecurity threats. However, cybersecurity and privacy must be integrated in order to effectively—most effectively protect those valuable assets.

The Department of Homeland Security has taken multiple steps, including several during my 3½-year tenure to integrate privacy into the DHS cybersecurity programs. First, as the Chairman noticed, DHS has thoroughly integrated the Fair Information Practice Principles into all of its programs, including cybersecurity. The FIPPs are eight interdependent principles that create a framework for how information may be used and shared in a manner that protects privacy: Transparency; individual participation; purpose specification; data minimalization; use limitation; data quality and integrity; security; and accountability and auditing.

DHS has furthermore been very transparent about its cybersecurity capabilities. For example, DHS published several privacy impact assessments, or PIAs, detailing pilot programs and information sharing among and between different entities, including a pilot program with the National Security Agency and an information-sharing program with the defense industrial base.

The Department engaged privacy advocates and private-sector representatives on its cybersecurity activities through a Federal advisory committee subcommittee, multiple meetings with advocates, and with Congressional testimony such as before this committee.

The Department has already hired multiple cybersecurity privacy professionals in order to embed them into the infrastructure at DHS. These privacy professionals review and provide comments and insight into cybersecurity standard operating procedures, statements of work, contracts, and international cyber information-sharing agreements. These privacy professionals also provide cyber-specific privacy training to the cybersecurity analysts to supplement the privacy training required for DHS employees and contractors.

Furthermore, an important tenet of the FIPPs is the concept of accountability. Given the importance of the DHS mission in cybersecurity, the DHS Privacy Office conducted a privacy compliance review in late 2011. My office found that the cybersecurity program was generally compliant with the requirements outlined with cybersecurity privacy impact assessments. This compliance review is available in the DHS Privacy Office website, as are all the privacy documents referenced in my written testimony.

Since I left DHS, I know through public knowledge that the Department continues to work to embed privacy protections into its cybersecurity activities. For example, its advisory committee, the Data Privacy and Integrity Advisory Committee, issued a robust paper for DHS to consider when implementing information-sharing pilots and programs with other entities, including the private sector. Furthermore, in January 2013, DHS published a thoughtful and comprehensive privacy impact assessment covering the enhanced cybersecurity surfaces, also known as ECS—we have a lot of acronyms, and I am sorry about that—ECS is voluntary program based on the sharing of indicators of malicious cyber activity between DHS and participating commercial service providers.

The information-sharing implementation standards described in the ECS PIA are concrete examples of privacy by design and should well position DHS to effectively implement the increased information sharing mandated in the 2013 Executive Order. In addition, just this week, the Department announced that it will deploy EINSTEIN 3 accelerated, known as E3A, network intrusion prevention capabilities on Federal Government networks as a managed security service provided by ISPs, rather than placing the entire response on the Federal Government.

DHS will share threat information it receives through E3A consistent with its existing policies and procedures. The way E3A is structured should enhance privacy, protect the Federal civilian Executive branch departments and agencies, and provide a nimble response to the evolving cyber threat.

The continued integration of privacy and cybersecurity is crucial for effective cybersecurity protections. In my 15 years, it is clear that privacy integration into the operational aspects of any activity makes the program both more effective and more likely to protect privacy. I believe DHS has appropriately and effectively integrated privacy and cybersecurity, both in its Federal Executive responsibilities and as an information-sharing responsibility.

Thank you for the opportunity to appear before you this afternoon. I am happy to take any questions.

[The prepared statement of Ms. Callahan follows:]

PREPARED STATEMENT OF MARY ELLEN CALLAHAN

APRIL 25, 2013

Chairman Meehan, Ranking Member Clarke, distinguished Members of the subcommittee, thank you for the opportunity to appear before you today. My name is Mary Ellen Callahan. I am a partner at the law firm of Jenner & Block, where I chair the Privacy and Information Governance practice and counsel private-sector clients on integrating privacy and cybersecurity. From March 2009 to August 2012, I served as the chief privacy officer at the U.S. Department of Homeland Security (DHS or Department). I have worked as a privacy professional for 15 years, and have National and international experience in integrating privacy into business and Government operations. I am appearing before this subcommittee in my personal capacity, and not on behalf of any other entity.

As this subcommittee knows, the United States' critical infrastructure, including Government assets, face significant cybersecurity threats. Cybersecurity and privacy must be integrated in order to most effectively protecting valuable assets. Furthermore, if done right, increased cybersecurity (with appropriate standards and procedures) also means increased privacy.

The Department of Homeland Security has taken multiple steps to integrate cybersecurity and privacy as part of the Department's cybersecurity mission. In fact, DHS has integrated privacy into its cybersecurity program since the EINSTEIN program was launched in late 2003. Shortly thereafter, the Department published one of the its first Privacy Impact Assessments (PIA) on EINSTEIN 1 (a network flow system), detailing the privacy protections that DHS embedded into its cybersecurity program from the beginning, and being transparent about those protections.[1] In 2008, DHS conducted a PIA on the second iteration of the DHS cybersecurity program, EINSTEIN 2 (adding an intrusion detection capability).[2] These PIAs exem-

[1] EINSTEIN 1, developed in 2003, provides an automated process for collecting computer network security information from voluntary participating Federal executive agencies. It works by analyzing network flow records. Even though DHS was not required to do a PIA given no personally identifiable information (PII) was being collected, DHS conducted a PIA (DHS/NPPD/PIA/001) on EINSTEIN 1 in September 2004 for transparency, available at: *http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein.pdf.*

[2] As with EINSTEIN 1, EINSTEIN 2 passively observes network traffic to and from participating Federal Executive Branch departments and agencies' networks. In addition, EINSTEIN 2 adds an intrusion detection system capability that alerts when a pre-defined specific cyber

plify the concept of "privacy by design" and are important foundational considerations for a large operational department like DHS.

I. DHS INTEGRATION OF PRIVACY PROTECTIONS INTO ITS CYBERSECURITY PROGRAMS

During my 3½-year tenure at DHS, we further integrated privacy into the DHS cybersecurity programs in several ways.

1. Integration of the Fair Information Practice Principles into DHS Cybersecurity Programs.—As noted below, DHS has thoroughly integrated the Fair Information Practice Principles (FIPPs) into its cybersecurity programs. The FIPPS are the "widely-accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy."[3]

The FIPPs are eight interdependent principles that create a framework for how information may be used and shared in a manner that protects privacy: Transparency; individual participation; purpose specification; data minimization; use limitation; data quality and integrity; security; and accountability and auditing.[4] During my tenure, my office worked tirelessly to integrate the FIPPs into all DHS programs, including cybersecurity.

2. Transparency.—DHS has been very transparent about its cybersecurity capabilities. During my tenure, DHS published several PIAs detailing pilot programs and information sharing among and between different Government entities. First, DHS discussed via PIA a 12-month proof of concept to determine the benefits and issues presented by deploying the EINSTEIN 1 capability to Michigan State government networks managed by the Michigan Department of Information Technology.[5] Shortly thereafter, DHS completed both a classified and unclassified PIA for the "Initiative Three Exercise"[6] of the Comprehensive National Cybersecurity Initiative."[7] In the Initiative Three Exercise, DHS engaged in an exercise to demonstrate a suite of technologies that could be included in the next generation of the Department's EINSTEIN network security program, such as an intrusion prevention capability. This demonstration used a modified complement of system components then being provided by the EINSTEIN 1 and EINSTEIN 2 capabilities, as well as a DHS test deployment of technology developed by the National Security Agency (NSA) that included an intrusion prevention capability. The DHS Privacy Office worked with DHS and the NSA to be as transparent as possible with the Exercise, including naming NSA (and its role in the Exercise) expressly in the PIA.

In early 2012, DHS published a PIA on its information-sharing pilot with the Defense Industrial Base;[8] after 180 days and a series of evaluations of its effectiveness, the PIA was updated to reflect the establishment of a permanent program to enhance cybersecurity of participating Defense Industrial Base entities through information-sharing partnerships. The permanent program was announced via PIA shortly before my departure.[9]

Furthermore, one of my last acts as Chief Privacy Officer was to approve a comprehensive PIA that described the entire National Cybersecurity Protection Sys-

---

threat is detected and provides the US–CERT with increased insight into the nature of that activity. The May 2008 PIA (DHS/NPPD/PIA–008) is available at: *http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf*.

[3] *National Strategy for Trusted Identities in Cyberspace,* April 2011, available at: *http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf*.

[4] DHS adopted the eight FIPPs as a framework for Privacy Policy on December 29, 2008; see DHS Privacy Policy Guidance Memorandum 2008–01, available at: *http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf*.

[5] *Privacy Impact Assessment Update for the EINSTEIN 1: Michigan Proof of Concept,* February 19, 2010, (DHS/NPPD/PIA–013) available at: *http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_einstein1michigan.pdf*.

[6] *US–CERT: Initiative Three Exercise Privacy Impact Assessment (unclassified),* March 18, 2010, (DHS/NPPD/PIA–014) available at: *http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3.pdf*.

[7] See *http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative* for a description of all 12 cybersecurity initiatives.

[8] *Privacy Impact Assessment for the National Cyber Security Division Joint Cybersecurity Services Pilot (JCSP),* January 16, 2012, (DHS/NPPD/PIA–021) available at: *http://www.dhs.gov/xlibrary/assets/privacy/privacy_nppd_jcsp_pia.pdf*. (N.B., this PIA has been retired with the release of the ECS PIA in January 2013, referenced below).

[9] *Privacy Impact Assessment Update for the Joint Cybersecurity Services Program (JCSP), Defense Industrial Base (DIB)—Enhanced Cybersecurity Services (DECS),* July 18, 2012, (DHS/NPPD/PIA–021(a)) available at: *http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-update-nppd-jcps.pdf*. (N.B., this PIA update has been retired with the release of the ECS PIA in January 2013, referenced below).

tem (NCPS), a programmatic PIA that explains and integrates all the NPPD/Cybersecurity and Communication (CS&C) cyber programs in a holistic document, rather than the previous patchwork PIAs that were snapshots in time of CS&C capabilities.[10] This NCPS PIA helps provide a comprehensive understanding of the CS&C cybersecurity program, further increasing transparency.

3. Outreach and engagement with advocates and private-sector representatives.—The Department engaged privacy and civil liberties advocates and private-sector representatives about its cybersecurity activities in several ways. First, as part of the *Cyberspace Policy Review* conducted by the administration in 2009,[11] the Department met with privacy and civil liberties advocates and academicians (at a Top Secret/SCI level) to discuss the Advanced Persistent Threat landscape, and Government response. That ad hoc meeting led to the creation of a subcommittee of DHS' Federal Advisory Committee Act-authorized committee, the Data Privacy and Integrity Advisory Committee (DPIAC).[12] The members and the experts on the DPIAC subcommittee (including privacy and civil liberties advocates, academicians, and private-sector representatives) were briefed frequently at the Top Secret/SCI level. After my departure, the DPIAC subcommittee produced an excellent report on integrating privacy into the DHS information-sharing pilots and programs, discussed below.

In addition to the systematic engagement of advocates, academicians, and private-sector representatives through the DPIAC subcommittee, DHS also discussed its embedded privacy and cybersecurity protections in several public fora, including Congressional testimony,[13] public articles,[14] and multiple public presentations before the DPIAC on DHS cyber activities.[15]

The DHS Privacy Office (and NPPD) also frequently met with privacy advocates to discuss cybersecurity considerations, either when a new program or initiative was announced, or during the quarterly Privacy Information for Advocates meetings instituted in 2009.[16]

4. Dedicated Cyber Privacy Personnel.—To be engaged and be able to effectively integrate privacy protections, the Department has hired multiple cyber privacy professionals. These cyber privacy professionals focus on integrating the FIPPs of purpose specification, data minimization, use limitation, data quality and integrity, and security systematically into NCSD activities. For example, the Sen-

---

[10] *National Cybersecurity Protection Program Privacy Impact Assessment,* July 30, 2012, (DHS/NPPD/PIA–026) available at: *http://www.dhs.gov/sites/default/files/publications/privacy/privacy-pia-nppd-ncps.pdf.*

[11] *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,* 2009, available at: *http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.*

[12] The DHS Data Privacy and Integrity Advisory Committee provides advice at the request of the Secretary of Homeland Security and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within the DHS that relate to PII, as well as data integrity and other privacy-related matters. The committee was established by the Secretary of Homeland Security under the authority of 6 U.S.C. § 451 and operates in accordance with the provisions of the Federal Advisory Committee Act (FACA) (5 U.S.C. App).

[13] See, e.g., *The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting Our National and Economic Security,* Joint Committee Hearing before Senate Committee on Homeland Security and Governmental Affairs and Senate Committee on Commerce, Science, and Transportation, March 7, 2013 (testimony of Secretary Janet Napolitano); *DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure,* Hearing before House Committee on Homeland Security, March 13, 2013 (testimony of Deputy Secretary Jane Holl Lute); *Examining the Cyber Threat to Critical Infrastructure and the American Economy,* Hearing before House Committee on Homeland Security, March 16, 2011 (testimony of NPPD Deputy Under Secretary Philip Reitinger).

[14] See, e.g., *Securing Cyberspace While Protecting Privacy and Civil Liberties,* Homeland Security Blog (by Secretary Janet Napolitano), April 2, 2013, available at: *http://www.dhs.gov/blog/2013/04/02/securing-cyberspace-while-protecting-privacy-and-civil-liberties; Op-Ed: A Civil Perspective on Cybersecurity,* (Jane Holl Lute and Bruce McConnell), WIRED, February 14, 2011, available at: *http://www.wired.com/threatlevel/2011/02/dhs-oped/all/.*

[15] See, e.g., on March 18, 2010, Deputy Assistant Secretary for Cybersecurity and Communications Michael A. Brown presented to DPIAC on computer network security and related privacy protections in DHS, including the Department's role in the CNCI (focusing on the DHS Privacy Office's work on PIAs for EINSTEIN 1, EINSTEIN 2, and the proof-of-concept pilot project of the EINSTEIN 1 capabilities with the U.S. Computer Readiness Team and the State of Michigan), the National Cyber Incident Response Plan (NCIRP), and the National Cybersecurity and Communications Integration Center, US–CERT, DHS I&A, and the National Cybersecurity Center; on July 11, 2011, the Senior Privacy Officer for NPPD Emily Andrew described how her office was integrated into the NPPD structure.

[16] See *DHS Privacy Office Annual Report,* July 2009 to June 2010 at 66 for a discussion of the Privacy Information for Advocates quarterly meetings, available at: *http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2010.pdf.*

ior Privacy Officer for the National Protection and Program Directorate (reporting to the Directorate leadership) was hired in August 2010; she has a dedicated privacy analyst on-site with CS&C and both are integrated into planning and implementation processes. In the DHS Privacy Office, there has been a liaison with NPPD cybersecurity organizations since the first EINSTEIN PIA was written; currently that position is Director, Privacy and Technology. This Director of Privacy and Technology was, for a period of time, embedded at the NSA as part of the development of the enhanced relationship between the NSA and DHS.[17]

When I was Chief Privacy Officer, I actively participated in numerous cybersecurity policy planning organizations within the Department.

5. Involvement and Coordination on Standard Operating Procedures, and Operational Aspects of DHS Cybersecurity Activities.—As part of its mission to implement the FIPPs and to integrate privacy protections into DHS cybersecurity activities, DHS privacy professionals review and provide comments and insight into cybersecurity Standard Operating Procedures (SOPs) (including protocols for human analysis and retention of cyber alerts, signatures, and indicators for minimization of information that could be PII), statements of work, contracts, and international cyber-information sharing agreements.

6. Cyber-specific Privacy Training for Cybersecurity Analysts and Federal Privacy Professionals.—These cyber privacy professionals provide cyber-specific privacy training to cybersecurity analysts to supplement the privacy training required for DHS employees and contractors. In my opinion as a privacy professional, the more relevant and concrete you can make privacy training, the more likely the audience will understand and incorporate privacy protections into their daily activities, thus increasing personal accountability.

During my tenure, the Department also engaged in a year-long Speakers Series for members of the Federal Government community to discuss privacy and cybersecurity issues, and their impact on Federal operations.[18] The Federal Government-wide access to the Speakers Series helped enhance awareness of the cybersecurity and privacy issues, along with providing an interagency communications channel on privacy and cybersecurity questions.

7. Accountability of the Cybersecurity Program Through Privacy Compliance Review.—An important tenet of the FIPPs is the concept of accountability—periodically reviewing and confirming that the privacy protections initially embedded into any program remain relevant, and that those protections are implemented.

While I was DHS Chief Privacy Officer, I instituted "Privacy Compliance Reviews" (PCRs) to confirm the accountability of several of DHS's programs.[19] We designed the PCR to improve a program's ability to comply with assurances made in PIAs, System of Records Notices, and formal information-sharing agreements. The Office conducts PCRs of on-going DHS programs with program staff to ascertain how required privacy protections are being implemented, and to identify areas for improvement.

Given the importance of the DHS mission in cybersecurity, the DHS Privacy Office conducted a Privacy Compliance Review in late 2011, publishing it in early 2012.[20] The DHS Privacy Office found NPPD/CS&C generally compliant with the requirements outlined in the EINSTEIN 2 PIA and Initiative 3 Exercise PIA. Specifically, NPPD/CS&C was fully compliant on collection of information, use of information, internal sharing and external sharing with Federal agencies, and accountability requirements.

My office made five recommendations to strengthen program oversight, external sharing, and bring NPPD/CS&C into full compliance with data retention and training requirements. NPPD agreed with our findings and, as I understand it, has taken multiple steps to address our recommendations. For example, in response to one of the recommendations, the NPPD Office of Privacy now conducts quarterly reviews of signatures and handling of personally identifiable information. These reviews have provided increased awareness to US–CERT Staff and

---

[17] *Memorandum of Agreement Between The Department of Homeland Security and The Department of Defense Regarding Cybersecurity,* September 2010, available at: *http://www.dhs.gov/xlibrary/assets/20101013-dod-dhscyber-moa.pdf.*

[18] See *DHS Privacy Office Annual Report, July 2011–June 2012* at 27 for a discussion of the four-part Speakers Series, available at: *http://www.dhs.gov/sites/default/files/publications/privacy/Reports/dhs__privacyoffice__2012annualreport__September 2012.pdf.*

[19] See id., *DHS Privacy Office Annual Report, July 2011–June 2012* at 39–40 for a detailed discussion of Privacy Compliance Reviews.

[20] *Privacy Compliance Review of the EINSTEIN Program,* January 3, 2012, available at: *http://www.dhs.gov/xlibrary/assets/privacy/privacy__privcomrev__nppd__ein.pdf.*

has helped to build positive working relationships with cyber analysts and leadership. This is important in continuing to integrate cybersecurity and privacy, by understanding the impact of each.

In addition, as this subcommittee knows, the DHS Chief Privacy Officer has unique investigatory authorities, therefore in the unlikely event that something went awry in the future, the Chief Privacy Officer can investigate those activities.[21]

II. DHS CONTINUES TO INTEGRATE PRIVACY PROTECTIONS INTO ITS CYBERSECURITY PROGRAMS

Since I left DHS, I know through public information that the Department continues to work to embed privacy protections in its cybersecurity activities.

A. DPIAC Cybersecurity Report

The DPIAC issued a robust advisory paper for DHS to consider when implementing information-sharing pilots and programs with other entities, including the private sector.[22] The report addresses two important questions in privacy and cybersecurity—"what specific privacy protections should DHS consider when sharing information from a cybersecurity pilot project with other agencies?" and "what privacy considerations should DHS include in evaluating the effectiveness of cybersecurity pilots?"

The DPIAC report supported in large part what DHS had been doing with regard to privacy protections incorporated in its cybersecurity pilots and programs. DPIAC recommended the following best practices when sharing information from a cybersecurity pilot project with other agencies: Incorporate the FIPPs into cybersecurity activities; develop and implement clear data minimization rules and policies; provide employees and public users of Federal systems notice and transparency of the collection, use, and sharing of information for cybersecurity purposes; when engaging in information sharing that includes PII or content of private communications, information sharing should be limited to what is necessary to serve the pilot's purposes (with defined limits on law enforcement, National security, and civilian agency sharing); have more robust safeguards for information from private networks; define data retention policies to keep records no longer than needed to fulfill the purpose of the pilot; and integrate privacy by design and privacy-enhancing technologies whenever possible.

This type of insight from privacy advocates, academicians, and private-sector representatives will enhance DHS' considerations of privacy-protective options when sharing cybersecurity information.

B. Enhanced Cybersecurity Services PIA

Furthermore, in January 2013, DHS published a thoughtful and comprehensive PIA covering the Enhanced Cybersecurity Services (ECS), a voluntary program based on the sharing of indicators of malicious cyber activity between DHS and participating Commercial Service Providers.[23] The purpose of the program is to assist the owners and operators of critical infrastructure to enhance the protection of their systems from unauthorized access, exploitation, or data exfiltration through a voluntary information-sharing program. ECS is intended to support U.S. critical infrastructure, however, pending deployment of EINSTEIN intrusion prevention capabilities, ECS may also be used to provide equivalent protection to participating Federal civilian Executive branch agencies.[24]

The ECS PIA is exemplary of how to integrate privacy protections into cybersecurity programs, particularly when engaging in information sharing with the private sector. This ECS PIA is the culmination of all of the hard work that I summarized above, including the DPIAC cybersecurity report.

---

[21] 6 U.S.C. § 142(b). See ibid., *DHS Privacy Office Annual Report, July 2011–June 2012* at 40 for a discussion of the DHS Chief Privacy Officer investigatory authorities.

[22] *Report from the Cyber Subcommittee to the Data Privacy and Integrity Advisory Committee (DPIAC) on Privacy and Cybersecurity Pilots, Submitted by the DPIAC Cybersecurity Subcommittee,* November 2012, available at: *http://www.dhs.gov/sites/default/files/publications/privacy/DPIAC/dpiac_cyberpilots_10_29_2012.pdf.*

[23] Privacy Impact Assessment for the Enhanced Cybersecurity Services (ECS), January 16, 2013, DHS/NPPD/PIA028, available at: *http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf.*

[24] This PIA consolidates and serves as a replacement to the two PIAs I mentioned earlier: DHS/NPPD/PIA–021 *National Cyber Security Division Joint Cybersecurity Services Pilot PIA,* published on January 13, 2012, and the DHS/NPPD/PIA–021(a) *National Cyber Security Division Joint Cybersecurity Services Program (JCSP), Defense Industrial Base (DIB)—Enhanced Cybersecurity Services (DECS)* PIA Update, published on July 18, 2012.

It is clear DHS continues to embed privacy protections into cybersecurity activities. The information sharing and implementation standards described in the ECS PIA are concrete examples of privacy by design, and should well position DHS to effectively implement the increased information sharing mandated by the February 12, 2013 Executive Order on Improving Critical Infrastructure Cybersecurity.[25]

C. EINSTEIN 3 Accelerated (E³A) PIA

In addition, just this week, the Department announced that it will deploy EINSTEIN 3 Accelerated (E³A) network intrusion prevention capabilities on Federal Government networks as a Managed Security Service provided by Internet Service Providers (ISPs), rather than placing the entire response on the Federal Government.[26]

The use of ISPs as a Managed Security Service is noteworthy from a privacy perspective for several reasons. First, the coordination and collaboration of the "best of breed" Federal classified and unclassified capabilities combined with the nimbleness (and proprietary capabilities) of the private-sector ISPs will allow a more robust response to evolving cybersecurity threats. It is an important recognition by DHS that Federal cybersecurity programs did not need to re-invent cybersecurity protections when defending Federal Government networks, but could supplement existing commercial intrusion prevention security systems to provide a more robust prevention and detection regime for the Federal civilian Executive branch.

Second, integrating cybersecurity threat detection and intrusion prevention will allow DHS to better detect, respond to, or appropriately counter, known or suspected cyber threats within the Federal network traffic it monitors, which helps protect the target systems from unauthorized intrusions (and therefore implements the security FIPP). It is important to emphasize—E³A monitors only select internet traffic either destined to, or originating from, Federal civilian Executive branch departments and agencies (commonly known as .gov traffic). This data minimization and segregation is also privacy-protective; the ISP Managed Security Service can be compartmentalized to affect only .gov traffic. The participating agencies will identify a list of IP addresses for their networks and both CS&C cybersecurity analysts and the ISPs verify the accuracy of the list of IP addresses provided by the agency. CS&C SOPs are followed in the event of any out-of-range network traffic is identified and the ISP removes any collected data to prevent any further collection of this network traffic. This too is a privacy-protective approach, further confirming that the only impacted traffic is Federal civilian Executive branch departments and agencies.

DHS will share cyber threat information it receives through E³A consistent with its existing policies and procedures (which have been thoroughly reviewed by the Department's cyber privacy professionals). In accordance with the SOPs and information-handling guidelines, all information that could be considered PII is reviewed prior to inclusion in any analytical product or other form of dissemination, and replaced with a generic label when possible, again protecting privacy. The way E³A is structured should enhance privacy, protect the Federal civilian Executive branch departments and agencies, and provide a nimble response to the evolving cybersecurity threat.

III. INTEGRATION OF PRIVACY PRINCIPLES INTO CYBERSECURITY IS CRUCIAL FOR EFFECTIVE CYBERSECURITY PROGRAMS

The continued integration of privacy and cybersecurity is crucial for effective cybersecurity protections. In my experience based on 15 years as a privacy professional as both outside counsel and chief privacy officer at DHS, it is clear that integrating privacy into the operational aspects of any activity makes the program both more effective and more likely to protect privacy. For example, providing tailored training, and engaging the analysts or employees in the field facilitates the integration of privacy into daily operations. Ex ante review of programs and anticipating issues such as unintended uses, data minimization, and defined standards for information sharing are also important to confirm privacy protections are working throughout the life cycle of information collection. Embedding privacy protections into SOPs and information-handling guidelines help to further the goal of the project while assuring that privacy protections are systematically integrated into a

[25] *Executive Order on Improving Critical Infrastructure Cybersecurity,* available at: *http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.*

[26] *Privacy Impact Assessment for EINSTEIN 3—Accelerated (E³A), April 19, 2013 (DHS/PIA/NPPD–027), available at: http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/PIA%20NPPD%20E3A%2020130419%20FINAL %20signed.pdf.*

program or service. Finally, transparency is the cornerstone for any privacy program to succeed.

These privacy-by-design factors are important any time an organization incorporates privacy into a new program, but they are particularly important with an operational cybersecurity program such the DHS National Cybersecurity Protection System which continuously counters emerging cybersecurity threats and applies effective risk mitigation strategies to detect and deter these threats. Integrating privacy from the beginning—and periodically testing to confirm that the integration continues—is the only way to effectively protect cybersecurity and privacy. In fact, if done right, increased cybersecurity also means increased privacy.

To address threats and minimize the impact on Federal facilities and critical infrastructure, key agencies and critical infrastructure companies must share information about cybersecurity threats. That said, such information sharing must occur in a thoughtful, clearly-designed process that also minimizes the impact on individual privacy. I believe that DHS has appropriately and effectively integrated privacy and cybersecurity both in its Federal Executive branch responsibilities and in its information-sharing responsibilities as articulated in the ECS and related cybersecurity PIAs. Currently, I advise private-sector clients that this privacy-by-design approach should be taken to most effectively combat cybersecurity threats by both increasing cybersecurity protections and protecting privacy.

Thank you for the opportunity to appear before you this afternoon. I would be happy to take any questions you may have.

Mr. MEEHAN. Thank you, Ms. Callahan.

The Chairman now recognizes Ms. McGuire for your testimony.

STATEMENT OF CHERI F. MCGUIRE, VICE PRESIDENT, GLOBAL GOVERNMENT AFFAIRS & CYBERSECURITY POLICY, SYMANTEC

Ms. MCGUIRE. Chairman Meehan, Ranking Member Clarke, and distinguished Members of the subcommittee, thank you for the opportunity also to testify today on behalf of Symantec corporation. We are the largest security software company in the world, with over 31 years of experience in providing security, storage, and systems management solutions. With more than 21,000 employees and operations in more than 50 countries, protecting critical infrastructure, Government, and citizens' data is core to our mission and our business.

My name is Cheri McGuire. I am the vice president for global government affairs in cybersecurity policy, where I lead a team that addresses the global public policy agenda for the company, including data integrity, critical infrastructure protection, cybersecurity, and privacy issues.

At Symantec, we are committed to assuring the privacy, security, availability, and integrity of our customers' information. Too often, security is portrayed as being in conflict with or somehow undermining privacy. However, in the digital world, nothing could be further from the truth, because your privacy is only as secure as your data. Criminals and hackers, many of whom are well-funded and highly skilled, have built a business model based on their ability to steal and monetize personal information.

Recent efforts to improve the Nation's cybersecurity posture have recognized that privacy and security must be addressed in tandem. Symantec supports an approach that allows to us share threat indicators and related non-PII within industry and within Government.

Now, I would like to talk briefly about today's threat landscape. As we briefed the committee last week, our latest internet security threat report noted that, in 2012, approximately 93 million identities were exposed through hacking, theft, and simple user error.

We also found that there was a 42 percent rise in targeted attacks, an increasing number which are directed at small businesses.

Finally, we saw a 58 percent rise in attacks designed to go after mobile devices. Simply put, every year, threats are increasing and becoming more sophisticated. Sharing actionable threat and vulnerability information is an essential element to combating threats like these. As a general rule, we believe that voluntary information-sharing programs are the best way to develop trusted partnerships to achieve the best results. That trust is weakened when Government information-sharing mandates are imposed on industry.

In order for information sharing to be effective it must be shared in a timely manner with the right people or organization and with the understanding that, as long as an entity shares information in good faith, it will not face legal liability.

In addition, the Government must have the proper tools and authorities to disseminate information effectively. We were pleased that the Executive Order the President signed in February and legislation passed in the House last week sent a clear message to the Government that sharing actionable information for cybersecurity purposes with the private sector is both a priority and a necessity.

Information sharing on cyber threats happens in a number of ways designed to protect our customers and their data. We get information from a myriad of sources, from our customers, our partners, the Government and our network—and through our network, called the global intelligence network of 69 millions attack sensors.

The information itself can be high-level threat data, details about a particular incident or attack, data signatures or other types of metadata. All of this data is then aggregated and analyzed, and during that process, we remove PII. Using this data, we develop machine-level signatures and other identifying information about specific pieces of malware and other threats. We also regularly publish analyses of attacks as well as white papers on current and future threat factors.

In closing, Symantec is deeply committed to securing the privacy and security of our customers' information. I hope that my testimony today has provided some insight into how we protect our customers' privacy and share threat information with our various partners while also balancing that with the need for robust cybersecurity. Thank you, again, for the opportunity to testify today, and I am happy to answer any questions you may have.

[The prepared statement of Ms. McGuire follows:]

PREPARED STATEMENT OF CHERI F. MCGUIRE

Chairman Meehan, Ranking Member Clarke, and distinguished Members of the subcommittee, thank you for the opportunity to testify today on behalf of Symantec Corporation.

My name is Cheri McGuire and I am the vice president for global government affairs and cybersecurity policy at Symantec. I am responsible for Symantec's global public policy agenda, including cybersecurity, data integrity, critical infrastructure protection (CIP), and privacy. In this capacity, I work extensively with industry and Government organizations, including serving from 2010 to 2012 as chair of the Information Technology Sector Coordinating Council (IT SCC)—one of 16 critical sectors identified by the President and the U.S. Department of Homeland Security (DHS) to partner with the Government on CIP and cybersecurity. I also serve as a board member of the Information Technology Industry Council, the TechAmerica Commercial Policy Board, and the U.S. Information Technology Office (USITO) in

China, and am a past board member of the IT Information Sharing and Analysis Center (IT–ISAC). Prior to joining Symantec in August 2010, I was director for critical infrastructure and cybersecurity in Microsoft's Trustworthy Computing Group. Before joining Microsoft in 2008, I served in numerous positions at DHS, including as acting director and deputy director of the National Cyber Security Division and U.S. Computer Emergency Readiness Team (US–CERT).

Symantec is the largest security software company in the world, with over 31 years of experience in developing internet security technology. We are the global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information and identities. We protect more people and businesses from more on-line threats than anyone in the world. Symantec has developed some of the most comprehensive sources of internet threat data through our Global Intelligence Network (GIN). Comprised of approximately 69 million attack sensors, the GIN records thousands of events per second and covers over 200 countries and territories 24 hours a day, 7 days a week. It allows us to capture world-wide security intelligence data that gives our analysts an unparalleled view of the entire internet threat landscape, including emerging cyber attack trends, malicious code activity, phishing, and spam.

Symantec also maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 51,000 recorded vulnerabilities (spanning more than 2 decades) from over 16,000 vendors representing over 43,000 products. Every day we process more than 3 billion e-mail messages and more than 1.4 billion web requests across our 14 global data centers. In short, if there is a class of threat on the internet, Symantec knows about it.

At Symantec, we are committed to assuring the privacy, security, availability, and integrity of our customers' information. Too often security is portrayed as being in conflict with or somehow undermining privacy. In the digital world, nothing could be further from the truth, because your privacy is only as secure as your data.

We welcome the opportunity to provide comments as the committee continues its important efforts to bolster the state of cybersecurity while protecting privacy in the United States and abroad. In my testimony today, I will provide the subcommittee with:

- our latest analysis of the threat landscape as detailed in the just-released Symantec Internet Security Threat Report (ISTR), Volume 18;
- our core privacy principles;
- an overview of the current information-sharing environment; and
- a summary of how we ensure privacy when we share threat information.

TODAY'S THREAT LANDSCAPE

We rely on technology for virtually every aspect of our lives, from driving to and from work, to mobile banking, to securing our most critical systems. As the use of technology increases so do the volume and sophistication of the threats. At Symantec, it is our goal to ensure that we are thinking ahead of the attackers. Looking at the current threat landscape is not enough—we must also keep our eyes on the horizon for evolving trends.

In the latest Symantec Internet Security Threat Report (ISTR), we detail that in 2012, approximately 93 million identities were exposed through hacking, theft, and simple error. That is 93 million individuals whose personal information is now potentially for sale in the black market—93 million people who are at risk for credit card fraud, identity theft, and other illegal schemes.

We also found that there was a 42 percent rise in targeted attacks last year.[1] It is almost certain that this trend will continue in the coming years. Conducting successful targeted attacks requires attackers to do research about the organizations they are seeking to penetrate, and often about specific people who work there. Attackers will mine the internet for information about how a company does business and use what they learn to craft personalized attacks designed to gain access to its systems. Once they gain access, they will move within a system, collecting information and staging data for exfiltration—the unauthorized transfer or release of data from a computer or server—to their own computers. Attackers can spend weeks and months covertly moving around a victim's system, collecting e-mail, personal data, documents, intellectual property, and even trade secrets.

We also saw a sharp rise in the exploitation of mobile malware. Last year, mobile malware increased by 58 percent, and 32 percent of all mobile threats attempted to steal personal information, such as e-mail addresses and phone numbers. Attacks

[1] *Symantec Internet Security Threat Report* XVIII, April 2013. *http://www.symantec.com/security_response/publications/threatreport.jsp*.

on mobile devices will almost certainly continue to rise as we become ever more reliant on these devices to perform our daily activities, such as working, banking, shopping, and social networking.

Another alarming finding was the rise of attacks on small and medium-size businesses. In 2012, 50 percent of all targeted attacks were aimed at businesses with fewer than 2,500 employees, and the largest growth area for targeted attacks was aimed at businesses with fewer than 250 employees. Thirty-one percent of all attacks targeted them, up from 18 percent the year before. This likely stems from the fact that unlike large enterprises, smaller businesses often do not have the resources to install adequate security protocols, making them an easier target for attackers. Yet many of these small companies subcontract or work for larger companies—and thus hold intellectual property and trade secrets coveted by attackers. As one of our security engineers likes to say, while every subcontractor may sign a strict non-disclosure agreement, the attacker who is sitting on that small company's system is not bound by it.

In sum, whether they are attacking our computers, mobile phones, or social networks, cyber-criminals are looking to profit by spying on us or stealing our information. Our best defense is strong security, education, and good computer hygiene.

PRIVACY AND SECURITY GO HAND-IN-HAND

At Symantec, we are guided by the following privacy principles: First, customers should be empowered to decide how their personal information is used, and informed what—if anything—will be done with it. Second, privacy protections must be integrated into the development of products or services and not added as an afterthought. Finally, we all need to be proactive in protecting privacy—absent strong security, information is vulnerable.

Criminals and hackers—many of whom are well-funded and highly skilled—have built a business model based on their ability to steal and monetize personal information. There is an entire criminal eco-system that trades in stolen personal information, as well as the tools and technology that allow them to steal more. Some of these criminal enterprises are so sophisticated that they provide 24/7 customer support, and offer guarantees that the stolen information they provide is valid.

In the face of this criminal threat, it should go without saying that strong security is essential to securing our personal data and private information. Simply put, if your data is not secure, then neither is your privacy. And, if you do not take steps to secure your own personal information, or the companies to which you entrust it do not do so, you are gambling with your privacy. When it comes to personal data, security measures and data protection are not an infringement on privacy but instead are the foundations of protecting it.

Recent efforts to improve the Nation's cybersecurity posture—whether legislative initiatives or Executive branch actions—have recognized that privacy and security must be addressed in tandem. The various bills in the House and the Senate have taken different approaches, but in the information-sharing area there is broad agreement that both the Government and the private sector need to be able to share cybersecurity information for cybersecurity purposes. This view also is shared by many prominent civil society organizations. Reaching consensus on the precise parameters of those terms is where complications have arisen. Symantec supports an approach that allows us to share threat indicators and related non-Personally Identifiable Information (PII) within industry and with the Government. In our view, companies should receive legal protection for sharing appropriate information with other companies or civilian agencies, and we believe that data minimization standards are a reasonable approach.

THE CURRENT INFORMATION-SHARING ENVIRONMENT

Globally, there are many different information-sharing models, ranging from voluntary programs to regulatory mandates to ad hoc arrangements to contractual agreements. Sharing can be Government-to-Government, business-to-business, and between Government and business. As a general rule, we believe that voluntary programs—which of course leave space for contractual and ad hoc arrangements—are the best way to develop trusted partnerships to achieve the best results. In the United States, we have a voluntary framework based on the National Infrastructure Protection Plan (NIPP).[2] The NIPP, as refined by the recent Presidential Decision

[2]National Infrastructure Protection Plan (2009), *http://www.dhs.gov/xlibrary/assets/NIPP__Plan.pdf*.

Directive 21, establishes 16 critical infrastructure sectors and identifies a sector-specific Federal agency for each.[3]

Within each sector, there are Government Coordinating Councils (GCC) and Sector Coordinating Councils (SCC). Nearly all sectors also have chartered Information Sharing and Analysis Centers (ISAC), operational entities that are tied to industry and serve as a focal point for voluntary information sharing. The level of trusted partnership and engagement among the GCCs, SCCs, and ISACs varies from sector to sector. Symantec has a long and successful history of participation and leadership in various multi-industry organizations as well as public-private partnerships in the United States and globally, including the National Cyber-Forensics & Training Alliance (NCFTA), the IT–ISAC, the Industry Botnet Group Mitigation Initiative, and many others.

Effective sharing of actionable information among the public and private sectors on cyber threats, vulnerabilities, and incidents is an essential component of improving cybersecurity. It is important to recognize that information sharing is not an end goal, but rather is one of a number of tools to enhance the security of IT systems. Good information sharing provides situational awareness so that appropriate protective and risk mitigation actions can be put into place. In order for information sharing to be effective, information must be shared in a timely manner, must be shared with the right people or civilian organizations, and must be shared with the understanding that so long as an entity shares information in good faith, it will not face legal liability.

The NCFTA provides a good example of how private industry and law enforcement partnerships can yield real-world success. NCTFA is a Pittsburgh-based organization that includes more than 80 industry partners—from financial services and telecommunications to manufacturing and others—working with Federal and international partners to provide real-time cyber threat intelligence.

The IT–ISAC is another example of a successful public-private partnership. The group's primary purpose is to allow organizations to exchange information about security threats and vulnerabilities. Member companies report information concerning security problems that they have or solutions to such problems that they have found. Members also participate in National and homeland security efforts to strengthen IT infrastructure through cyber threat information sharing and analysis. The IT–ISAC also has an industry-funded representative that works at the National Cybersecurity & Communications Integration Center (NCCIC) to facilitate real-time information sharing and response.

One of the most successful U.S. public-private partnerships has been cybersecurity exercises. The level of engagement and resources brought to bear from the Government and industry to jointly plan and develop scenarios, define information-sharing processes, and execute the exercises has been unprecedented. When done right, the lessons learned from these exercises have been invaluable to both industry and Government to help improve response plans and improve preparedness for future incidents.

In addition, the Government must have the proper tools and authorities to disseminate information effectively. I have seen too many instances of the Government releasing information on cyber threats days and sometimes weeks after a threat has been identified. In many of these cases, by the time the Government releases the information it often has little use because the private sector has already identified and taken actions to mitigate the threat. There is no single solution that will eliminate these delays, but various legislative proposals move us one step closer to eliminating some of the legal barriers that currently impede sharing. Moreover, the Executive Order (EO) the President signed in February 2013 sent a clear message to the Government that sharing information with the private sector is both a priority and a necessity.[4]

Further, we also support an incentive-based approach to information sharing. There is no doubt that businesses can gain a competitive advantage by not disclosing information to their competitors. However, a well-incentivized program of collaboration can help offset those disadvantages and keep the information flowing freely. We also need to address policies that discourage businesses who would be willing to share information but choose not to because of fear of prosecution. There-

---

[3] The 2009 National Infrastructure Protection Plan *(http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf)* identified 18 critical infrastructure sectors. Presidential Decision Directive 21 (Critical Infrastructure Security and Resilience, signed February 12, 2013) revised that to 16. See *http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil*.

[4] See Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," 78 Fed. Reg. 11739 (February 19, 2013).

fore, liability protections are necessary to improve bi-directional information sharing.

As with any partnership, information sharing is founded upon and enabled by trust. That trust is weakened when Government information-sharing mandates are imposed on industry. Enhanced self-interest and a flexible approach are more likely to improve information sharing than Government mandates.

PROTECTING PRIVACY AS WE SHARE THREAT INFORMATION

At Symantec, we understand the vital importance of sharing information for cybersecurity awareness and response. We recognize that information stored on our servers is sensitive, confidential, and often personal in nature. Therefore, we take very seriously our role in safeguarding our customer's personal information and go to great lengths to ensure that personal information remains private.

Information pertaining to customers such as credit card information, addresses, or other PII is not shared under any circumstances unless we are compelled by law, following appropriate due process. In addition, we comply with the Payment Card Industry Data Security Standard and follow specific rules under our privacy program to ensure that we collect only data that is proportionate for the purposes for which it is collected, and that is relevant and necessary for the services provided.

Information sharing on cyber threats happens in a number of ways and for various reasons. We get information from myriad sources—from our customers, our partners, the Government, and our network of sensors. The information itself can be high-level threat data, details about a particular incident or attack, data signatures, or other information. All of this data is then aggregated and analyzed, and during that process we remove PII. The resulting work product can range from machine-level signatures or identifying information for a specific piece of malware to a quick analysis of a particular attack to a published white paper on current and future threat vectors. This work product can then be provided to our customers and partners in both the private sector and the Government, depending on the particular parameters of the sharing agreement.

In some cases, the communication is purely bilateral—a customer provides us information about activity on its system (either manually or through an automated sensor), and we report back on what we see happening. Other times we share it broadly, including sometimes publicly, but only after removing any PII to ensure that the report cannot be linked to a particular individual or customer. When we share reports on attack trends or publish white papers on particular threats, PII is removed as part of long-standing policy and we only share information directly related to the cyber threat. We have legal and organizational safeguards to ensure that information is only disclosed to the intended partners and only used for the expressed purpose.

In closing, Symantec is deeply committed to securing the privacy and security of our customer's information. Thank you again for the opportunity to testify, and I will be happy to answer any questions you may have.

Mr. MEEHAN. Thank you, Ms. McGuire.

The Chairman now recognizes Ms. Pearson to testify.

STATEMENT OF HARRIET P. PEARSON, PARTNER, HOGAN LOVELLS

Ms. PEARSON. Thank you very much, Chairman Meehan, Ranking Member Clarke, and Members of the subcommittee.

My name is Harriet Pearson. I am a partner in the Hogan Lovells law firm, where I focus on cybersecurity and privacy law. From November 2000 until July 2012, I served as the IBM corporation's chief privacy officer and security counsel, and I have been engaged in this area of privacy and security since the mid-1990s.

Thank you for the opportunity to participate in today's hearing on how we in the United States in the business community and in Government can protect our critical infrastructure from cyber-based threats while safeguarding individual privacy.

Let me start with the observation that the relationship between cybersecurity and privacy is complex, as we have heard. On the one hand, cybersecurity that protects data from intrusion, theft, and

misuse obviously is a significant privacy safeguard that cannot be understated. On the other hand, some cybersecurity measures that monitor access and use of systems and digital networks can implicate the collection of personal information, or PII, where data can be linked to individuals and thus raises some privacy concerns.

Understanding that relationship and integrating privacy into cybersecurity has never been more important. As we have heard and as the committee well knows, the threat is out there. There are risks, and the risks come in multiple forms, particularly for those businesses that are part of the critical infrastructure and that have to take these measures. The private sector's role in this respect is vital. You know that the critical information, much of it and much of the most valuable intellectual property of our society are owned and managed largely by the private sector. Therefore, the steps that companies take to safeguard their most precious possessions and assets and figuratively to lock up and secure their premises are very significant. Increasingly companies are stepping up to that challenge and taking those measures.

Let me articulate a couple of, or give you a couple of examples of the kinds of measures that might implicate some level of collection or access to potentially personal information. There are some measures, such as systems and network monitoring; you have to know what is going on in your systems. You might have to access and collect some personal information. Background checks, more of us are bringing our own devices and hooking them up to sensitive or important networks, and you have to make and take safeguards. Supply chain and vendor networks need to be secured, and sometimes you need information. Information sharing, as has been discussed with Government and other entities in the private sector, might also at times implicate some kind of personal information and thus steps need to be taken.

My recommendations for how these concerns can be addressed start with the premise that it can be addressed. There are responsible ways and many organizations are already taking those steps in the business community. Some suggestions for how and observations on how organizations are taking those steps include, first, we have talked already on the panel, and Chairman and Ranking Member talked about the Fair Information Practice Principles, or the FIPPs. That is an important acronym to keep in mind in my view. Applying the FIPPs is what privacy professionals do in the United States all day long, every day, in many situations. Applying FIPPs to information sharing and other cybersecurity measures and steps is absolutely critical.

Second, one of the most foundational elements of the FIPPs is this notion of transparency, articulating what you are doing, educating and being open about the steps taken, not of course to the degree that it compromises the important security measures that need to be taken but articulating it so that there is some understanding of the measures and that there is some ability to say, hmm, what is going on, let's have a conversation about it in the democratic tradition of the United States.

Third, we have in this country a tradition of creating codes of conduct, voluntary measures that once organizations buy into them and engage in them, actually become quite important as a measure

of establishing base lines of behavior in business. I endorse the development of voluntary codes of conduct for the privacy-sensitive deployment of certain cybersecurity measures and programs that are common enough to warrant such effort. Examples of this might include information-sharing codes of conduct in which organizations that engage in information-sharing partnerships with each other and with Governmental agencies developed and commit to adopt privacy-sensitive practices such as the one that Ms. McGuire mentioned.

Another example is the new work that is being undertaken by NIST, as mandated by the recently-issued Executive Order on critical infrastructure cybersecurity, to develop a privacy—to develop a cybersecurity framework. As you know, NIST is consulting with multiple stakeholders on the development of this kind of framework, and the committee can play an important role in asking about and looking at the kind of privacy for consideration built into that framework.

Finally, through law, the expectations, responsibilities, and legal protections for privacy when data is shared or requested by Government in particular need to be clear, and there have been certain legislation enacted through this house that have clarified the role and some important progress and language has been included in that and further efforts by Government and industry leaders outside of this kind of legislation will also be useful to educate and enable stakeholders involved in these activities to design privacy in information sharing and related activities.

Thank you for the opportunity to appear before you today, and I will be happy to take questions.

[The prepared statement of Ms. Pearson follows:]

PREPARED STATEMENT OF HARRIET P. PEARSON

APRIL 25, 2013

Chairman Meehan, Ranking Member Clarke, and Members of the subcommittee, my name is Harriet Pearson and I am a partner in the Hogan Lovells law firm, where I focus on cybersecurity and privacy law.[1] From November 2000 until July 2012 I served as the IBM Corporation's chief privacy officer and security counsel.

Thank you for the opportunity to participate in this hearing on how we in the United States can protect our critical infrastructure from cyber-based threats while safeguarding individual privacy.

The relationship between cybersecurity and privacy is complex. On the one hand, cybersecurity that protects data from intrusion, theft, and misuse obviously is a significant privacy safeguard. On the other hand, cybersecurity measures that monitor access and use can implicate the collection of personal information (or data that can be linked to individuals), and thus raises privacy concerns.

Organizations of all types increasingly are taking steps to protect themselves and the people that rely on them from cyber-based threats. Cyber threats come from many different sources. The risk to information systems and the data that resides or travels on them can come from activists, criminals, or spies. Most of the time, these bad actors attack from outside the company; sometimes, they strike from within. Frequently they are enabled by the carelessness or inattention of otherwise well-meaning individuals who leave the digital analog of the front door open for easy

[1] My professional service includes membership on the advisory boards of the Future of Privacy Forum and the Electronic Privacy Information Center. I was a founding and long-time member of the board of the International Association of Privacy Professionals. I also serve on the American Bar Association president's Cybersecurity Legal Task Force, co-chair the Cybersecurity Law Institute of the Georgetown University Law Center, and was a member of the CSIS Commission on Cybersecurity for the 44th Presidency. The views I express are mine only, and are not offered on behalf of Hogan Lovells or its clients, or other organizations.

entry. And sometimes there is no affirmative attack at all, as in case where a system malfunction occurs or sensitive data is lost or misdirected by accident—presenting risks that are still quite significant if such information gets into the wrong hands.

Since the critical infrastructure and the most valuable IP of our society are owned and managed largely by the private sector, the steps companies take to safeguard their most precious possessions and figuratively to lock their doors, close their windows, and make sure only authorized people and things cross the threshold are exactly the steps needed to improve cybersecurity for society at large. Sharing information about observed threat patterns and vulnerabilities with other companies and with appropriate authorities is also part of the mix. This is akin to participating in a neighborhood watch that involves proactive and collaborative engagement with law enforcement.

While adoption of cybersecurity defenses will, as I noted, serve to protect personal data (indeed, there can be no data privacy without sufficient security, including cybersecurity), some of the defense techniques may require the monitoring or collection of personal information, and thus implicate privacy concerns.

- *First, there is network and system monitoring*.—Experts agree that in order to detect and defend against cyber attacks, organizations should be aware of how their information networks and IT systems are behaving. Such monitoring typically is focused on non-personal information such as malware indicators, bad IP addresses, and network flow data. Of course, the more specifically one monitors, and potentially records, activity, the more potential there is that personal data will be part of the information reviewed and/or collected.
- *The next issue is that of background checks*.—Not all cyber-defense measures involve cyber tactics. Organizations frequently find it prudent to conduct background checks—at times quite extensive—on individuals with access to certain sensitive systems and data. By definition, background checks require the collection and use of personal information.
- *A new aspect of data security arises from the "Bring Your Own Device" phenomenon*.—An increasing number of organizations are allowing their workforce to use personally-owned smartphones, PCs, and other devices. The steps organizations take to secure such devices and the data that might be stored on them often involve access to personal data.
- *Steps taken to strengthen supply chain and vendor security may also raise privacy issues*.—Security-conscious enterprises understand that the weakest link in their organization may lie outside their formal control. Measures imposed on their vendors and suppliers may require those third parties to conduct background checks and share other information that has privacy implications.
- *Information sharing with third parties and Government agencies means that personal information may be shared*.—Finally, but importantly, experts agree that rapid and preferably automated cross-organizational sharing of cyber threat information is essential to help detect and defend against cyber attacks. And as Members well know, given the recent passage of H.R. 624, the Cyber Intelligence Sharing and Protection Act, there can be significant privacy issues raised by such sharing.

While each of these areas of cybersecurity techniques raises privacy concerns, those concerns can be addressed responsibly.

First, consistent with the well-known Fair Information Practice Principles,[2] data collection should be thoughtfully limited; used only for the purpose of security or other carefully considered and approved purposes; retained only for as long as needed for security and other legitimate purposes; and shared only with those that need the data for security or other carefully considered and approved purposes, with accompanying limitations on their sharing, use, and retention. These are concepts that privacy professionals in American business apply every day, and close collaboration between privacy professionals and security personnel at companies is essential to ensure that the security/privacy balance is correct and that Fair Information Practice Principles are applied to design privacy into cybersecurity programs.

Second, there should be transparency as to the cybersecurity measures that organizations, especially operators of critical infrastructure, increasingly are using. Transparency is fundamental to the Fair Information Practice Principles. When im-

[2] The U.S. privacy framework is based on underlying principles of fairness known as "Fair Information Practice Principles" or "FIPPs," which were first developed in the United States in the 1970s and have since influenced every privacy law, regulation, or code of conduct adopted in this and many other nations. The Fair Information Practice Principles focus on empowering individuals to exercise control over personal information that pertains to them, and on ensuring that measures are taken to achieve adequate data security.

plemented, it reassures individuals that the processing of information that relates to them is not being done in secret, thus enabling them to pursue any recourse available if necessary.

As it relates to cybersecurity measures, transparency would include encouraging companies that are deploying network and systems monitoring to disclose their use of such measures (not in sufficient detail as to defeat their operations, of course, but in enough detail that individuals know about the systems monitoring the use of workplace technologies and the like). The more we inform and educate each other about how cybersecurity systems work, and how privacy considerations are addressed in their design and implementation, the more these measures are demystified.

Third, I endorse the development of voluntary codes of conduct for the privacy-sensitive deployment of cybersecurity measures and programs that are common enough to warrant such effort. Examples might include information-sharing codes of conduct, in which organizations that engage in information-sharing partnerships with each other and with Governmental agencies develop and commit to adopting privacy-sensitive practices. Another example is new work by the National Institute for Standards and Technology as mandated by the recently-issued Executive Order on Improving Critical Infrastructure Cybersecurity, to develop a voluntary Cybersecurity Framework that includes consideration of privacy. As you know, NIST will be consulting with stakeholders in both Government and industry as it develops the Framework. This subcommittee can keep the focus on privacy issues by showing interest in, and requesting to see, how privacy is integrated into NIST's and others' cybersecurity efforts.

Finally, the expectations, responsibilities, and legal protections for privacy when data is shared with or requested by Government need to be clear. Legislation that clarifies the rules surrounding information sharing is a valuable first step, and it is encouraging to see that the privacy issues associated with information sharing have been discussed and that language addressing these issues has been included in the legislation proposed in this Congress. Further efforts by Government and industry leaders, outside of new legislation, will also be useful to educate and enable stakeholders involved in these activities to design privacy into information sharing and related activities.

Thank you for the opportunity to appear before you today and to present my thoughts on how we can achieve a meaningful balance between privacy and protecting the United States' critical infrastructure.

Mr. MEEHAN. Thank you, Ms. Pearson.

Thanks, each of you on the panel, for helping us to set the table on this issue. Let me begin, because I think that may be one of the places for us to begin to draw the parameters around this issue to get to the places where we think the real crux of the privacy issues find themselves.

I was struck your testimony, Ms. Callahan, where you said, if done right, increased cybersecurity with appropriate standards and procedures also means increased privacy.

Ms. McGuire, you testified that security is portrayed as being in conflict with or somehow undermining privacy; in the digital world, nothing could be further from the truth.

Ms. Pearson, you discussed a little bit where there may be some sort of conflicts, but at the same time, there are some steps being taken. You talked about FIPPs.

Maybe that is a good place to start. I would like your general observations, each in order, about what you believe are the important steps that are being taken to create the privacy protections while we enable information to be shared and maybe specifically what FIPPs is and how that enhances this ability. Ms. Pearson or others, if you have an area in which you find you say "but," don't tell hesitate to tell us what the "but" is.

Ms. Callahan, I will recognize you.

Ms. McGuire, Ms. Pearson, in order.

Ms. CALLAHAN. Thank you very much, sir.

My testimony with regard to increased cybersecurity can enhance increased privacy goes to the FIPP of security because the information has to be kept secure; it has to be kept contained. Ms. McGuire testified about 93 million exposed identities, and those people did not have the FIPPs to protect them in that circumstance. But what is important is the parenthetical that you read of mine, which is, you have to have the appropriate standards, procedures, and safeguards within that in order to protect that information.

Mr. MEEHAN. Can you take one moment and tell me 93,000 people——

Ms. CALLAHAN. Ninety-three million identities.

Mr. MEEHAN [continuing]. Did not have the FIPPs. Would you explain what you mean by that?

Ms. CALLAHAN. It is Ms. McGuire's number, but I think it involves data breaches, ma'am.

Ms. MCGUIRE. The number was 93 million identities that were lost or stolen in 2012, and that could be through any number. It could be cyber attacks, laptops stolen, et cetera.

Mr. MEEHAN. Okay.

Ms. CALLAHAN. So the concept of unauthorized access, whether we are talking about it as a laptop or a device, as Ms. Pearson talked about, or an actual cyber attack, where an organized cyber criminal is taking the information. In that circumstance, not all FIPPs prevent. That is my point about security as an important element to the protection of privacy, because if you can't keep the information secure, then you can't have privacy, but you can enhance it if indeed you have the proper safeguarding.

Mr. MEEHAN. So, in other words, even though the Government may not be getting that information for 94 million people, it is already out there in not only the private sector but out there in the world of criminality and otherwise.

Ms. CALLAHAN. That is correct. It could be as much as that. That we need to mitigate that and address that going forward.

Mr. MEEHAN. Ms. McGuire.

Ms. MCGUIRE. So I think it might be useful for me to take a little bit about Symantec's sort-of, our privacy principles, and we have three of those: First, that we believe that customers should be empowered to decide how their personal information is used and informed what, if anything, will be done with it; and second, that privacy protections must be integrated into the development of products and services and not added as an after-thought; and finally, that we all need to be proactive in protecting our own privacy, and absent strong security, as I said before, information is vulnerable. We take a number of steps as a company to secure the privacy, the PII information of our customers and our partners and those are tied directly to the FIPPs, as Ms. Callahan discussed, as well as a number of internal policies, privacy policies, and privacy impact tools that we use across our company. So I think it has to be a multi-pronged approach, both with informing customers as well as developing your own internal policies and practices to safeguard that personally identifiable information.

Mr. MEEHAN. Where do you come down on the industries developing personal policies, but where does the Government come in on creating policies that the industry needs to adhere to?

Ms. MCGUIRE. Well, I think that, as Ms. Pearson talked about, this notion of voluntary or codes of conduct that have been developed over time, the adoption of those can be quite useful, as well as internationally developed standards that many times those codes of conduct form the basis for as it moves through the standard development process.

Mr. MEEHAN. I am worried about the changing nature of the threat and whether or not we will be able to create consistent, sort-of, this is today's standard, it may be less relevant tomorrow if there are new technologies or new ways to get around it.

Ms. MCGUIRE. Well, I think you raise a very, very important point, and that is standards need to be flexible enough so that, as time evolves, the nature of the threat evolves, that they can evolve—the standard can evolve as well. Sometimes if they are written too tightly, they will constrict the ability to respond and deal with the next level of threat as it evolves.

Mr. MEEHAN. Thank you.

Ms. Pearson, my time is up, but your time is still ticking to answer and be responsive to any of the issues that were raised.

Ms. PEARSON. What I will say is that the Fair Information Practice Principles were developed in the United States over 30 years ago, and they are still as good today as they were back then. So that shows the power of having principles that can guide our behaviors. When it comes to identifying what kind of information you collect, if you are a business trying to protect your assets and your people and then share, there are some really foundational questions, which is: What am I doing, what am I collecting, do I really need to collect it? The answer may be, no, or the answer may be I do collect a lot of information so that I can identify patterns, so I can see abhorrent uses, so I can secure my networks. Once you decide on kind of a principle level, what are you collecting, the question then becomes: What do you need to share it, what exactly do you need to share? From my own experience and personal experience with my clients, I know that the vast majority of the information involved in addressing cyber threats has nothing to do with individuals. It is IP addresses. It is the signatures. It is very technical information. So when it comes time to share that information, that really is not a privacy-related concern. Where there might be information that relates to individuals, then the question becomes: Do you need to share it? How important is it to the mission involved or to the goal? Are there abilities to strip or share or amass or protect that information? That is really the question.

Operationally speaking, I see companies more and more being able to do that. I see innovation in the marketplace, American innovation on the part of the companies, like Ms. McGuire's and others, coming up the curve to help deal with that particular privacy issue and help address technical or operational or market measures. That is what I see.

Then, finally, as you deal with industry-to-Government, the question I think that you are all in an excellent place to address is: What will Government do with it? What will happen to it, and

what kind of assurances back and forth are in place to make predictable to the American people and to business what happens to that information, including protecting its confidentiality for privacy purposes as well as business confidentiality purposes?

Mr. MEEHAN. Thank you.

My time has expired, and now, at the suggestion of the Ranking Member, we are going to go out of order and recognize the gentlemen from Nevada, Mr. Horsford, for questioning.

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

Thank you to the Ranking Member, I appreciate the courtesy to our witnesses, and thank you for being here.

Just briefly, obviously, this is an important National security issue, and the need for qualified cybersecurity experts has grown at the same time. Everyone from our President to the GAO has said that we have to address this as a serious economic challenge, both in the public and private sectors.

Now it appears that our ability to meet the cybersecurity workforce needs of the Nation are not fully understood or fully quantified. Would you recommend that the Federal Government work with the private sector as well as training and educational institutions to address the problem of kind of the workforce areas of cybersecurity? If so, how?

Ms. MCGUIRE. So, really important this issue of workforce development and education and training for the future cybersecurity experts and workers of the future. Today, we have a number of public-private partnerships between industry and Government that have been quite effective. Unfortunately, they are not effective enough because the demand is so high for these types of high-skilled employees in the future, but things like the National Cybersecurity Alliance, the National Initiative for Cyber Education, that DHS and NIST and the Department of Defense and Commerce are leading, those are the kinds of efforts, as well as National Science Foundation's, Cyber Corps to train up that next generation.

We need more of those kinds of programs, frankly, in order to meet the challenge of this deficit. It really is a deficit that we have. I can tell you today, as a company, we have more than a thousand openings, a thousand job openings, for high-skilled engineers, and we could go across any number of high-tech companies as well as manufacturing and other industries, who cannot meet the challenge today. That really is impacting our country's economics moving forward.

Ms. CALLAHAN. I would note briefly the Secretary and Deputy Secretary have testified before this committee asking for such flexibility, and these initiatives that Ms. McGuire spoke about are helpful, but I think that we need to do more to really help buttress the cybersecurity options.

Ms. PEARSON. One thought on privacy aspects here, as I have worked with cybersecurity professionals, the best ones have taken training and have an enormous degree of sensitivity to the importance of privacy as they work on defending against attacks and also safeguarding information. So an element of cybersecurity curricula ought to be, and I believe it is in most of these programs, an element of data protection or privacy training as well.

Mr. HORSFORD. So gathering all of these, like you said, initiatives and public-private partnerships to know what is out there and what is working and where the gaps might be, steps this committee could take to move some ideas forward.

Let me also ask, as I said, cyber threats are both in the private and public sector. I am from Nevada, and we have a large number of facilities critical to National security. The Nevada National Test Site is in my district, for example, and is a critical component to National security efforts. Obviously, do you agree that we need to do everything we can to protect these facilities?

Ms. CALLAHAN. Yes, absolutely.

Ms. MCGUIRE. Yes.

Mr. HORSFORD. So my follow-up question is: In this budgetary environment, does the protection from cyber threats against our National security facilities need to be a budget priority?

Ms. MCGUIRE. We have stated during this uncomfortable period of sequestration and some of the cuts that are going on, that cybersecurity issues should be at the forefront and a priority to not be taking the scalpel to at this point in time. I think you can look at any number of reports, whether they are our report or others, as well as reports coming out of various agencies, that this is not the time to be putting our critical infrastructure, our National security apparatus at risk.

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

Thank you to the Ranking Member, again, for the courtesy.

Mr. MEEHAN. I thank the gentlemen for taking the time to join us today. I know he had conflicts in his schedule. It is deeply appreciated.

Also, for the record, I think we all share the genuine appreciation to assure the adequate funding for this very, very important area, although this is one of the areas, actually the budget was plussed up in this area, which was, in this day, a victory, where staying even is the new staying ahead; that was a good result.

At this moment, the Chairman now recognizes the gentleman from Montana, Mr. Daines.

Mr. DAINES. Thank you, Mr. Chairman.

I was—my last 12 years in the private sector before I came to Congress here in January was actually the cloud computing company that we took public in global operations. So we were very much in the midst of denial-of-service attacks and I guess living in the world you all live in every day.

We had a case one time where the Federal Government came asking for customer data regarding a threat to our National security; in fact, it was the Secret Service that approached us, and we refused to give the information up, saying this was customers' data; it was not our data, ultimately. The Secret Service moves quickly, and a subpoena came about 2 hours later, and then we had a process where we could hand the data over to investigate the situation.

What do you think is the minimum amount of data, talking about the balance of privacy and protecting our country and industry from cyber attacks, what is the minimum amount of data that you think we need to adequately trace back a cyber attack? I would love to get opinions on that.

Ms. MCGUIRE. So I think there is often a lot of questions around IP addresses and whether or not that is considered PII or not. In our view, IP addresses are really a pointer back to a specific threat, and they need to be aggregated with other information in order to actually resolve back to an individual. So, at the face value, because we get this question a lot, are IP addresses PII, and there is a little bit of a gray area there; sometimes they can be, but generally they are not. So I think this goes to the crux of the broader issue around attribution and the difficulty we have with attribution today because IP addresses are not generally static; there are constantly changing. So to your question around what is or isn't, it is not always clear, but I think if you have the proper standards and practices and policies in place to make sure that privacy or PII information and privacy is protected, that you are on the right side of the issue.

Ms. CALLAHAN. I would add, for the Department of Homeland Security, when I was there, the way they would address it is that there were these signatures or indicators that may or may not contain what could be personally identifiable information. Ms. McGuire mentioned IP address. There also may be other indications that could be personally identifiable information. So what the Department has done, due to its standard operating procedures, is to look at that and see whether or not that personally identifiable information needs to be shared or information that could be personally identifiable needs to be shared as part of the signature or indicator. If it does, then it has to be approved by a supervisor to make sure that it indeed is consistent with the SOP. So if it is necessary, that information will be shared, but you have to analyze it to make sure that it is not just being shared because it is easier.

Mr. DAINES. Ms. Pearson.

Ms. PEARSON. I agree with my colleagues. Most of the time, piecing together what happened or what is the source does not really require access to personally identifiable information, but sometimes it does. It is a little bit like detective work. I think you can avoid that kind of data to some degree, but sometimes, it is just embedded in systems. It is embedded in the kind of thinking you have to do. It is not just the digital detective work; sometimes you have to think about, for example, was somebody trying to—and this is an amalgam of client experiences I have had—is somebody trying to get at a system using a mix of physical as well as digital measures? So then the question becomes: Well, who had access, physically who had access? That is the kind of information that might be collected and might conceivably be shared with law enforcement because fundamentally most of this kind of activity we are talking about is against the law.

Mr. DAINES. Right. Let me ask you this, Wayne Gretzky made the famous comment, "skate to where the puck is going." In this very dynamic and world of innovation and break fix, and things change within minutes and hours; you talked a bit about technology that could be used to minimize data as it is coming in as it is relates to privacy. Where do you see that headed as—of course, we have had a lot of concerns from our constituents about the whole privacy issue, but where do you think this is all headed here when you make advancements in technology that can cost-effec-

tively minimize data, still allows us to investigate but yet protects the privacy of our constituents?

Ms. PEARSON. My own view is that the market speaks, and as the market looks for solutions like this, that protected security by either requesting or rewarding the ability to manage in mass data, then these solutions are technically feasible and have already been invented, frankly, and it is a matter of commercializing them, doing what you did, taking it to the market.

One thing to note, in my view also, is that we are here talking about homeland security issues, cybersecurity issues as it relates to that aspect, but there are so many other reasons that companies need to keep information secure and confidential. There are other sources of legal obligation. There are other sources of reputational issues.

Mr. DAINES. The forces of competition.

Ms. PEARSON. The forces of competition are absolutely there, and the innovations available to embed, whether it is cloud computing or in new ways of segmenting information on devices that we all carry and use these days, are available or are coming. It is a matter, I think, of pooling them.

Mr. DAINES. I know my time is up. I would love to have Ms. McGuire answer that if I could, Mr. Chairman.

Mr. MEEHAN. The Chairman would allow Ms. McGuire to share her instincts on this.

Ms. MCGUIRE. Thank you. I think there are—there is a lot of work being done in this area as far as innovation with moving to machine, really machine-to-machine readable data, so that people don't even get into the middle of this. It is about really identifying at the front end when the data is coming in what would be considered PII so that maybe a human never actually even looks at it. So I think that is certainly a direction that we need to go in when we are talking about this kind of information sharing for cybersecurity protection. That is, I think, is a major innovation the industry is moving towards today.

Mr. DAINES. Thank you.

Mr. MEEHAN. Thank you, Mr. Daines.

The Chairman now recognizes the Ranking Member, the gentlelady, Ms. Clarke.

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

I thank the panelists once again for bringing their expertise to bear on this very timely issue. There are two central privacy concerns when we talk about private-sector collaboration with the Government to stop cyber attacks, are over what information gets sent and who in the Government it is sent to. Various legislative approaches to these two questions have been quite controversial and is something we in Congress are still struggling to get right.

So I want to ask the panel three questions: How much minimization of the information should be required from the private sector side when sharing information? Does too much minimization place an undue burden on companies, and where is the right place in the Government for this sharing to occur?

Ms. CALLAHAN. Thank you very much, Ranking Member Clarke. The concept of minimization is an important tenant of the FIPPs and one that the DHS applied very consistently through its stand-

ard operating procedures when I was there, and I believe continues to do so. With that said, how much minimization is appropriate, necessary from the private sector? I don't think the question how much is—I think it is more to think about how to effectively and efficiently implement it, rather than putting the burden on the private sector to go through all these laborious steps, but if they address it, either through machine-to-machine readable that Ms. McGuire spoke about, or through other standard policies and procedures, like the Department has been implementing, which is kind of now like muscle memory in terms of how to implement it, I think it can be an effective tool in order to share timely information on threats without unduly burdening privacy.

Ms. MCGUIRE. From our perspective, we think that reasonable minimization standards or practices as are outlined in the FIPPs is appropriate and is not an undue burden for industry. At least from our perspective, we do that today.

As far as your question about where should the information-sharing relationship reside within the Government today, our view is that it should reside with the civilian agency and for a couple of reasons. One is, we believe that it sends the right message to our citizens and to other governments. We have a long tradition of—in this country of being a civilian-led government, and we also believe that the civilian agencies today have a framework in place to work with the private industry.

If you look at the level of investment over the last 10 years, that industry as well as Government has put into the public/private partnerships, for example, that DHS today is the focal point and lead for with the participation of the rest of the associated agencies as well as the Department of Defense, we believe that we should build on that foundation and not, you know, spend another 10 years trying to create something that, while we need improvements, we can utilize and build on today.

Ms. PEARSON. Let me add my perspective on this. In terms of data minimization, one thing to note would be that, by far, the majority, if not every single organization, the private sector that I have seen, no one is eager to open the door and hand over information to Government unless there is process of some sort, some rules around it. The gentleman spoke about a subpoena or some kind of legal structure, and I think the minimization of information to be handed over or to be shared or to be allowed to access to, a lot of that motivation is there already. So in terms of standards, I think educating and putting that thought process into, for example, the new NIST cybersecurity framework so that it is put in there as other elements are put in as a voluntary framework that we all know will be quite influential. I think is very important to send a signal and the expectation there.

Certain businesses and organizations in the private sector have more sophistication than others, and so I think as well for smaller and medium-sized businesses, particularly that thought process and the technology of how to do that, I think, will be perhaps more challenging than other large organizations, so that is an open issue that I don't have a solution for at this moment, but again, you know, I would point to it.

Then, finally, in terms of the right place or the central location, I guess my observation would be that in the last number of years that I have been working in this area, that there has been a collaboration among agencies as everyone has sorted through who has expertise, how do you go about doing this, how do you work with the private sector, and that collaboration today, while imperfect, no doubt, has been effective and has shown a regard for the mission and the objective over a regard for individual organizational dynamics, and that, I think, is the most important element to continue.

I share Ms. McGuire's general view of the importance of civilian-led engagement, but I also am cognizant of the fact that there have been collaborations that have been very effective and worthwhile that have been handled primarily through the military more or military agencies.

Ms. CLARKE. Very well. Thank you very much.

I yield back, Mr. Chairman.

Mr. MEEHAN. I thank the gentlelady.

The Chairman now recognizes the gentleman, the former prosecutor for Massachusetts, Mr. Keating.

Mr. KEATING. Thank you, Mr. Chairman, Ranking Member.

I just had a question. There has been a lot of discussion about the private-sector involvement, the Governmental involvement. To what extent are universities and colleges involved in dealing with this issue, trying to seek resolution, trying to do research, looking at programs? What is your experience about their involvement in this and how has that been utilized by either government or the private sector? Anyone?

Ms. CALLAHAN. I guess I will start. So, there is a great deal of research going on with cybersecurity and cybersecurity protections. There is also a lot of integration among the different colleges to help protect it. In addition, as you note, sir, the colleges themselves have potentially critical infrastructure information or research information that they will need to protect themselves. So, from the Department's perspective, they have been—they were—when I was there, and I think they have continued since I have left, continued to do outreach to try to help bolster both the cybersecurity training that Ms. McGuire spoke about but also to help bolster the research involved therein.

Ms. PEARSON. The additional observation I will make is that universities and colleges in our country are among the most privacy-sensitive organizations, particularly because they are Federally statutorily mandated to protect educational records, and so I think from a privacy side of the cybersecurity equation, they would be among the institutions I would say would be most sensitive to the aspects of what to do to monitor systems to, you know, protect information that way.

They also, as a group, happen to have access to some of the leading-edge innovation in intellectual property in this country, and so incenting them and helping universities identify their crown jewels and to encourage them to protect is, I think, an important attribute of what we are doing as a strategy and National strategy, and you know, I think that is important.

Mr. KEATING. I believe there is a middle ground myself that they could really occupy, where they don't have a commercial interest as much as some cyber, you know, some private-sector sides. The additional benefit of investing in universities will address one of the other issues that were brought up. As we are using and utilizing universities, we are going to have more trained people available in the workforce, so that is a major side benefit of doing that, so I just——

Ms. MCGUIRE. I would also just add that the academic institutions and universities have been involved in this information sharing for quite awhile now with their research and education networking, information sharing and analysis center, the REN–ISAC as it is called. It is actually a consortium of universities that share threat and other types of data amongst themselves so that they can help to bolster their own protections, and that has been in existence for over 10 years now. So I think it is important that we also make sure that they are a part of this information-sharing partnership as well moving forward.

Mr. KEATING. You know, I do believe there is a greater place for them in adopting some policies and using some of that innovation and some of the models that might be there.

Quick question. Let's assume there is a major cyber attack, attack on systems, something that would have a dramatic effect on our economy. Now, there will be a reaction to that. What would be the one thing you would not want to see Government react to perhaps that would be overreacting to such a major, major event, because there will be reaction when that happens, and there will be a suddenness if we don't move on our own ahead of time? What would be your greatest fear that Government would overreact in that kind of situation?

Ms. MCGUIRE. I think there is two. One is on the operational real-world side, which is that—and this goes back to that attribution question that we talked about earlier, that perhaps there might be some kind of defensive posture taken that is more detrimental as an outcome than the attack itself and perhaps targets the wrong systems or networks as part of that defense.

The second piece is really around policy, and that is that when we—when we see big events of other types in the past, we can often get a knee-jerk reaction in the development of policy or rules and regulations that may not, may not always be as conducive in the long run while they are trying to address the short-term issue to our ability to protect ourselves for the long term. So those are the two areas.

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

Mr. MEEHAN. Thank you, Mr. Keating.

The Chairman now recognizes the gentleman from Texas, Mr. Vela. No questions at this point in time. Thank you. I am very grateful for your taking the time to join us, Mr. Vela, and notwithstanding.

If the—no objection, I have a few follow-up questions on some issues that I would like to have you further clarify.

The panel has talked a number of times today about personally identifiable information sort of in the context of other questions, but I think there is a fundamental question: Just what do you be-

lieve personally identifiable information might be? Then, what is threat information, and how are they distinguished? Are there similarities? Help me to help others understand what you think those terms mean.

Ms. CALLAHAN. I guess I will go first. So, there is a kind of traditional definition of personally identifiable information which is associated with an individual, name, email address, social security number, telephone number, and that has traditionally been the definition of personally identifiable information. There has been an approach to broaden that for information that is identified or could be identified with an individual, and that is the current Federal definition of personally identifiable information, so you could have some liaison information with it.

In fact, the Federal Trade Commission, on a slight different note actually has now included IP address, MAC address associated with mobile devices and other information that is personally identifiable information in their rule on children's privacy. So it is kind of a little bit of a moving target.

With regard to Department of Homeland Security and how they think about personally identifiable information in the cyber context, they look at information, including IP address, and they presume that it is personal information, so this data mineralization process I spoke about earlier with the gentleman from Montana talks about let's presume that an email address or an IP address is personal information, is it necessary to be included in the signature or the threat information?

Mr. MEEHAN. Right.

Ms. CALLAHAN. It is a broad definition, and then the analysis is whether or not it should be included in the threat. But as my colleagues noted earlier, the vast majority of time, even that broad definition of personally identifiable information isn't necessary to include in the threat.

Mr. MEEHAN. Now, how about because we are watching—and I think there was some testimony. I know it was in the written testimony. We have seen a tremendous expansion in the amount of mobile devices that are now being used as back doors to that, so is that expanding on the amount of information that may be getting caught up in the net if we are starting to do more to look after protecting against violations that happen on personal devices?

Ms. MCGUIRE. Yeah. I think there is no question that the proliferation of different devices and ways for us to connect to the internet and to move our data around creates a larger attack surface, if you will, and more opportunities for the bad guys to access our personal information. So, you know, things like FIPPs and other kinds of policies to protect your private data, coupled with all of the necessary security that you need to have on all of those devices, they have to be done, done together to ensure, at least provide a level of assurance that your information and your privacy is secured.

Ms. PEARSON. So let's take a really concrete example. Let's say you are a business with a few thousand employees and you allow employees to use their smartphones or iPads, or you know, device and connect and do work, and let's say that somebody who operates your systems sees some weird behavior, and they say: Well, what

is going on? They look to see, and it is some of the source of that information, of that aberration is coming from a few of the devices that are hooked up to the network. What is collected is system information and device information to find out what is going on, what is the source of it. That is threat information. That is the kind of information, when you are in a business, you are collecting.

The next question is: Well, do you share it with anybody? Do you go to one of these information-sharing collaboratives with industry and then say: I have seen something; have you seen something? You compare notes. It is kind of like a Neighborhood Watch. You say, well, you know, this is kind of happening in my neck of the woods, my neighborhood.

Most of the information—all the information in that context is not identifiable information because you are just saying, well, I have got devices, and this is what I have seen. The question that turns it from threat information that is non-PII to personal information is if you have reason to say: Oh, and that device belonged to X.

Mr. MEEHAN. Why would you say that, though? Is there a circumstance where you would?

Ms. PEARSON. In a situation I just painted where you are trying to figure out what is going on, probably not. If there is reason to think that some—that whoever had that device needs to be contacted to be asked questions or maybe there was something going on, perhaps then there might be, which is why I think all of us in our remarks have talked about how the majority of information in the cyber context is not PII, but sometimes it might be, and then it becomes a matter of safeguarding and treating that information well.

That is, I think the danger of trying to overcircumscribe how this stuff works because it is very—it is complex, it is changing, the technology is changing, and the way to address these issues today is very different from what it was even a couple of years ago and it will change going forward.

Mr. MEEHAN. Go ahead and recognize my Ranking Member for some follow-up questions as well.

Ms. Clarke.

Ms. CLARKE. Thank you, Mr. Chairman.

You know, this is such a fascinating area that we are engaged with right now, and we are really just at the beginning of what can ultimately be a way of life for us because the technologies is ever-evolving, but I have a question about data breach information, obligations, rather.

When a company is hacked, what is its obligation to its customers? What is its obligations to its employees and its shareholders? Do you think that current law is sufficient to compel corporations to give their stakeholders the information they need? That is one question.

Then I want to ask another very important question because this is over time. So, over the past decade, we have witnessed an explosion in the usage of the internet for all aspects of everyday life. Networking technologies have now fully penetrated our civil society. Many are worried about the intended and unintended consequences of this. Some have talked about changing expectation of

privacy as a result of the internet. Many people have mused that no one will be able to run for President in the future due to the amount of information about us through social media, whether it is Facebook, LinkedIn, all of these things that reveal so much about us. Do you think that these technologies are changing how we think of our privacy? How do you see the internet affecting our conception of privacy in the future?

Ms. PEARSON. Really simple questions. Can I start?

Ms. CALLAHAN. Sure. Go ahead.

Ms. PEARSON. I will start with the second one first. That is the broad question, I think, of our time for those of us who work in this area daily. There is something—every realm, every type of new technology that has some implication for the collection management of information over time, starting with, you know, even before the camera, but the camera is kind of a modern era start of the technology cycle that has led us to camera to telegraph to telephone to video, et cetera, et cetera, prompts this question, and we as a society search for the answer, and we as an American society have come up with a unique blend of mechanisms, law enforcement, policies, norms to answer it for ourselves as a people.

This current era in which we live is a very rapid technology cycle, and the rapidity of it has challenged our whole concept. So while I resisted tweeting that I was coming in here, I will tweet on my way out, and it is, I think, the generation to come, the digital native generation will reflexively, I think, engage in this information sharing, to speak of another kind of information-sharing activity, much more normally and as regularly than we might. But I believe firmly, and I think there are studies that show it academically that the human psyche needs a zone of privacy, and it just needs to express itself in different ways, given the parameters of what we are living in.

So I firmly believe that despite some of the rhetoric around here, humans have, American—you know, in our American society, but globally, some sort of psychological need for a zone in which to express oneself, and you know, in our country, I think the challenge will be to reinvent that for the coming era and figure out what the laws and norms are around it.

Ms. MCGUIRE. I will take the first question on data breach first. Clearly, companies have a series of obligations to inform their customers, their employees, and their shareholders.

Today, however, we do have a patchwork of regulation around that. I think we have 48 different State laws, and that can be difficult for companies to scale to when they have experienced an unfortunate data breach issue. So having some commonality around what that reporting should be, I think, at least from our perspective, would be desirable.

On the second question around internet—the increasing use of internet and how it is changing and evolving our perceptions on privacy, there is no question that I think, as Ms. Pearson stated, that there is a big difference between, you know, the over-30 generation and the under-30 generation on how we perceive our privacy and our own information.

I was part of a panel a couple of weeks ago on privacy and security where we were discussing the changing nature of anonymity

on the internet and the role that that will play in regard to future views on privacy. So I think we are starting to see a huge evolution, if you will, just in how we are going to be thinking about these issues in the future.

Ms. CALLAHAN. If I could have two small points on both questions. You asked about data breach obligations, and I think it is worthwhile to note that the patchwork of State laws that Ms. McGuire mentioned involved a very narrow definition of personally identifiable information. So it would be first and last name, coupled with a sensitive identifier, such as social security number, but there can be many cyber breaches that may not reach the level of a data breach for notification.

Now, there is—so it is almost two different types of breaches, a cybersecurity incident and a data breach incident. With that said, there is guidance from the SEC that public companies should notify about if there has been an incident, but they also should notify whether or not there is a possibility or some sort of problems, and I think that is worth noting in terms of your shareholder question.

With regard to the internet, I think that the FIPPs of user control and transparency are going to be important tenets as we get into this kind of ubiquitous always on-line information. You should know what is being happening with information and how you as an individual can control it. I think that will help define privacy in the future.

Mr. MEEHAN. Well, I thank you. Let me ask one sort of closing question to the extent you feel comfortable answering it, because obviously as we work through, this is one example, although one of the critically important issues that we are dealing with as we try to find a framework for legislation that helps us find the very balance that we are exploring today. So, if you were in our shoes and you were writing the legislation, how would you look to write something that accommodates the concerns that we are sharing today? What would be in that legislation to help, you know, limit the sharing of PII but still encourage the ability for us to get the necessary threat information that we need to protect?

Then what kind of rules do you think we should be putting in place to encourage and give guidance to companies to allow them to feel comfortable doing information sharing, in fact, to encourage it, because part of the fear is if you have outliers that don't participate, as you have stated, the weakest link may be the avenue in, how do we make sure that we do the most to protect our system?

So, you are the legislators and we have got to go to draft, what would be included to address those issues? I will ask you to move across.

Ms. CALLAHAN. Well, thank you very much, and I am happy to be a legislator. I enjoyed my time in the Executive branch, but I look forward to being on your side. No, just kidding.

If I were writing the legislation, I would want to make sure that this—that the FIPPs were thoroughly integrated into the legislation, and we have spoken a lot about how effective that is and how it is a framework, and it is very flexible, and I think those are important tenets to put in there. We don't want to be too prescriptive, we don't want to be too specific, but we want to have the frame-

work and the concepts, and I think data minimalization from the information sharing is a very important tenet.

With regard to the types of rules to be put in place, FIPPs, obviously, but I will also say that the NIST cybersecurity framework that is currently going on with the Executive Order can be a very useful tool to help all the small- and medium-sized enterprises who are going to be sharing information as well as the large multinational ones have the same kind of baseline and not try to reinvent the wheel.

Ms. MCGUIRE. I largely agree with everything that Ms. Callahan has said, but I will just add that I think there is one or two additional pieces. In addition to the FIPPs components and building on the existing frameworks that we have in place today, those two key pieces are that civilian agency, as a lead, I think, are very important to ensuring that our citizens feel comfortable that their personal information is not somehow being used for purposes other than securing networks and systems, and also the legal liability issue for companies especially to feel comfortable to share information with the Government.

Today we are—we have a very laborious process. If we want to share something that is not part of a contractual arrangement that exists today, a business arrangement with Government agencies, that can take a lot of time, and oftentimes the information becomes stale.

Mr. MEEHAN. They say in a moment where we are talking microseconds sometimes about information being relevant to preventing a threat.

Ms. MCGUIRE. Yes. Information becomes stale very quickly, and so today we have to go through a series of internal privacy checks as well as legal checks and antitrust checks if we want to share with other companies even. As you can imagine, that takes a lot of time and resources when time is often of the essence.

Mr. MEEHAN. Thank you.

Ms. Pearson.

Ms. PEARSON. I also largely agree with my colleagues. The additional couple of points I would make is that as legislators, the oversight function that you have the ability to play should not be underestimated at all and should continue to be exercised, particularly in this area, to make sure that the agencies involved and the stakeholders involved are discharging for obligations here. I think that is very important.

Another point to make is that certainty is important. Certainty is important to business, of course, and I know from my service on, for example, the American Bar Association Cybersecurity Legal Task Force, which cuts across the entire bar association and other fora that, as a whole, the members of the bar who are counseling companies across the board, different industries, are coming off the curb, so to speak, on their understanding how the different laws here intersect with one another and work with another, whether it is antitrust or privacy or other things, and encouraging that kind of maturation, I think, for example, by holding briefings, by——

Mr. MEEHAN. Are you saying that they are beginning to understand the parameters and more effectively counsel their clients as to what they may or may not do?

Ms. PEARSON. It is a complex—as you noted before, it is a complex area of law, and the challenge with security and securing is that it implicates so many areas of law, current law and then a lot of the law that is coming. So what I see happening is more and more, you know, the defense industrial-based pilot, for example, was it a fantastically successful pilot? As involvement of industry broadens in the framework at NIST and the voluntary efforts, so is an additional expansion of individuals, particularly in the legal community who are starting to understand how to put all those pieces together, and so that should be encouraged, in my view.

Mr. MEEHAN. Well, I think we have time constraints, so I want to express my deep appreciation. I think we could go on with this hearing well into the evening hours, but I need to respect everybody's time, and I particularly appreciate the work that each and every one of you has done, not just in the preparation for this hearing, but your long period of service in what is a vital and important area now for our Nation as we move forward trying to find the right balance on this and the other questions that are relevant to the challenge that we face.

I don't think anybody denies or is running from the true nature of the very real threat that exists out there in the cyber world that is affecting people in so many different capacities, but I also am confident in our capacity to meet the challenge if we do it with enough forethought.

So I thank you for having very, very valuable testimony to this consideration as we work together as a committee to try to reach the right challenge in the bills that we will propose. There may be Members from the committee who have a question, and if they do and they submit it to you, I would ask that you do your best to try to respond in writing, if that should happen. But I thank you for your continuing work and I look forward to continuing dialogue as we move through on this very important issue.

I thank the Members of the committee. The committee now stands—subcommittee now stands adjourned.

[Whereupon, at 3:44 p.m., the subcommittee was adjourned.]