



MARCH 4, 2015

# INDUSTRY PERSPECTIVES ON THE PRESIDENT'S CYBERSECURITY SHARING PROPOSAL

HOUSE OF REPRESENTATIVES COMMITTEE ON HOMELAND SECURITY, SUBCOMMITTEE ON  
CYBERSECURITY, INFRASTRUCTURE, AND SECURITY TECHNOLOGIES

ONE HUNDRED AND FOURTEENTH CONGRESS, FIRST SESSION

---

## HEARING CONTENTS:

### *OPENING STATEMENTS*

**Rep. John Radcliffe (R-TX)** [\[view pdf\]](#)

Chairman, Subcommittee on Cybersecurity, Infrastructure, and Security Technologies

### *WITNESSES*

**Mr. Matthew J. Eggers** [\[view pdf\]](#)

Senior Director, National Security and Emergency Preparedness, U.S. Chamber of Commerce

**Ms. Mary Ellen Callahan** [\[view pdf\]](#)

Former Chief Privacy Officer, U.S. Department of Homeland Security

**Mr. Greg Garcia** [\[view pdf\]](#)

Executive Director, Financial Services Sector Coordinating Council

**Dr. Martin Libicki** [\[view pdf\]](#)

The RAND Corporation

### *WEBCAST:*

**Hearing Video**

<http://www.ustream.tv/recorded/59519723>

*COMPILED FROM:*

<http://homeland.house.gov/hearing/subcommittee-hearing-industry-perspectives-president-s-cybersecurity-information-sharing>

*\* Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*



Committee on  
**HOMELAND SECURITY**  
Chairman Michael McCaul

*Opening Statement*

March 4, 2015

**Media Contact:** April Ward  
(202) 226-8477

---

**Statement of Subcommittee Chairman John Ratcliffe (R-Texas)  
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies**

**“Industry Perspectives on the President’s Cybersecurity Information Sharing Proposal”**

**Remarks as Prepared**

The subcommittee meets today to hear from key stakeholders including industry, privacy advocates, and academia on the president’s cybersecurity information sharing proposal and recent cyber initiatives. Last week, the full committee heard testimony from the Department of Homeland Security’s top cyber officials on the growing cybersecurity threat and how this legislative proposal could enhance protection of our digital networks and Americans’ most personal information. Today, we turn to the private sector and look forward to hearing from our witnesses on what they think cyber threat sharing legislation should look like.

For years, the private sector has been on the front lines battling devastating cyber attacks from criminals, hackers, and nation-states such as Iran, China, Russia, and North Korea. Any cyber threat sharing legislation produced by Congress should enhance existing capabilities and relationships while establishing procedures to safeguard personal privacy.

Protecting privacy and the integrity of information is what compels us to act. The recent cyber breach of health insurance giant Anthem exposed the personal information of up to eighty million individuals—approximately one in four Americans—demonstrating that the quantity and sophistication of these attacks are only increasing. Just last week, Director of National Intelligence, James Clapper underscored this fact, stating that “[cyber] attacks against us are increasing in frequency, scale, sophistication and severity of impact” and “the methods of attack, the systems targeted, and the victims are also expanding in diversity and intensity on a daily basis.” He emphasized that privacy and the integrity of information are indeed at risk, stating, “in the future, we’ll probably see cyber operations that change or manipulate electronic information to compromise its integrity instead of simply deleting or disrupting access to it.”

Director Clapper also revealed that in 2014, America “saw, for the first time, destructive cyber attacks carried out on U.S. soil by nation-state entities,” confirming that Iran was behind a cyber attack against the Las Vegas Sands Corp., which is owned by a vocal supporter of Israel.

These breaches are becoming the norm, with attacks on Sony Pictures, Target, Home Depot, JP Morgan, and many others. FBI Director James Comey stated, “There are two kinds of big companies in the United States. There are those who’ve been hacked by the Chinese and those who don’t know they’ve been hacked by the Chinese.” Further, these attacks are not just affecting the largest businesses and financial institutions, but small and medium ones as well. As such, we need to pass legislation that facilitates the sharing of cyber threat indicators and contains robust privacy protections to improve collaboration between federal civilian agencies like DHS and the private sector.

The Department of Homeland Security’s National Cybersecurity and Communications Integration Center, or NCCIC, has been at the forefront working with the private sector to facilitate cyber threat sharing between the government and the private sector. NCCIC is a civilian cyber operations center with an embedded statutorily-required privacy office. In fact, both industry and privacy advocates support NCCIC, which was codified into law last year in bipartisan legislation produced by this committee.

NCCIC has been the lead civilian portal for cyber threat sharing between the private sector and the government and it is important that NCCIC and other civilian portals be the focus of any cyber threat sharing legislation.

Today, many companies still choose not to share cyber threat indicators with one another or NCCIC because they fear legal liability. Information about an attack experienced by one can enable another to fortify its defenses. Yet when this sharing does not occur, it leaves all of us more vulnerable because the same criminals can use the same tactics to target other companies, exposing even more Americans to having their private information compromised.

Past legislative attempts to improve cyber threat sharing between the private sector and government, and private sector-to-private sector, have failed in large part because they could not balance privacy protections with the need for industry to share cyber threat indicators. This Congress, I look forward to working with Chairman McCaul, Ranking Member Thompson, and Ranking Member Richmond to craft thoughtful cybersecurity legislation that achieves this balance.

I look forward to hearing from each of the witnesses in their respective fields about their opinions on how best this committee should move forward on drafting legislation to address these issues and what perspectives each of you have on the president’s recent legislative proposal and cyber initiatives.

Every generation faces monumental moments where their tenacity to overcome the challenges of the time are tested. Now is our time, as we move deeper into the digital age, to ensure that the cybersecurity challenges we face today are met with the same resolve shown by previous generations of Americans.

I want to thank the witnesses for testifying before this committee and I look forward to your testimony.

###



## Statement of the U.S. Chamber of Commerce

---

**ON: Industry Perspectives on the President's Cybersecurity  
Information-Sharing Proposal**

**TO: House Committee on Homeland Security  
Subcommittee on Cybersecurity,  
Infrastructure Protection, and Security Technologies**

**DATE: March 4, 2015**

---

1615 H Street NW | Washington, DC | 20062

The Chamber's mission is to advance human progress through an economic, political, and social system based on individual freedom, incentive, initiative, opportunity, and responsibility.

The U.S. Chamber of Commerce is the world's largest business federation representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations. The Chamber is dedicated to promoting, protecting, and defending America's free enterprise system.

More than 96% of Chamber member companies have fewer than 100 employees, and many of the nation's largest companies are also active members. We are therefore cognizant not only of the challenges facing smaller businesses but also those facing the business community at large.

Besides representing a cross-section of the American business community with respect to the number of employees, major classifications of American business—e.g., manufacturing, retailing, services, construction, wholesalers, and finance—are represented. The Chamber has membership in all 50 states.

The Chamber's international reach is substantial as well. We believe that global interdependence provides opportunities, not threats. In addition to the American Chambers of Commerce abroad, an increasing number of our members engage in the export and import of both goods and services and have ongoing investment activities. The Chamber favors strengthened international competitiveness and opposes artificial U.S. and foreign barriers to international business.

Positions on issues are developed by Chamber members serving on committees, subcommittees, councils, and task forces. Nearly 1,900 businesspeople participate in this process.

Matthew J. Eggers  
Senior Director, National Security and Emergency Preparedness, U.S. Chamber of Commerce  
House Homeland Security Committee  
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies  
Hearing titled “Industry Perspectives on the President’s Cybersecurity  
Information-Sharing Proposal”  
Wednesday, March 4, 2015

Good morning, Chairman Ratcliffe, Ranking Member Richmond, and other distinguished members of the committee. My name is Matthew Eggers, and I am a senior director of the U.S. Chamber’s National Security and Emergency Preparedness Department. On behalf of the Chamber, I welcome the opportunity to testify before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies regarding industry’s perspectives on the president’s cybersecurity information-sharing proposal.

The Chamber’s National Security and Emergency Preparedness Department was established in 2003 to develop and implement the Chamber’s homeland and national security policies. The department works through the National Security Task Force, a policy committee composed of roughly 200 Chamber members representing practically every sector of the American economy. The task force’s Cybersecurity Working Group, which I lead, identifies current and emerging issues, crafts policies and positions, and provides analysis and direct advocacy to government and business leaders. Industry’s interest in cybersecurity is healthy and expanding—individuals join the working group almost daily.

The need to address increasingly sophisticated threats against U.S. and global businesses has gone from an IT issue to a top priority for the C-suite and the boardroom. Chamber President and CEO Thomas J. Donohue recently said, “In an interconnected world, economic security and national security are linked. To maintain a strong and resilient economy, we must protect against the threat of cyberattacks.”

My statement highlights the successful rollout of the National Institute of Standards and Technology’s (NIST’s) *Framework for Improving Critical Infrastructure Cybersecurity* (the framework)<sup>1</sup> and the positive collaboration that many businesses and government entities have developed over the past several months, including the Chamber’s cybersecurity campaign—*Improving Today. Protecting Tomorrow*<sup>™</sup>.

I am also going to focus on policy issues—information-sharing legislation being the top legislative priority—that lawmakers and the administration need to diligently address. The information-sharing discussion puts too little emphasis on improving government-to-business sharing. The Chamber wants to expand government-to-business information sharing, which is progressing but needs improvement.<sup>2</sup>

---

<sup>1</sup> See [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework).

<sup>2</sup> The Chamber submitted in October 2014 similar comments to the National Institute of Standards and Technology (NIST) related to businesses’ awareness and use of the framework. See [http://csrc.nist.gov/cyberframework/rfi\\_comments\\_10\\_2014.html](http://csrc.nist.gov/cyberframework/rfi_comments_10_2014.html).

The framework is a good start, but more work is needed to push back against skilled attackers. Most small and midsize businesses (SMBs) tend to lack the money and personnel to beat back highly advanced and nefarious actors, such as organized criminal gangs and groups carrying out state-sponsored attacks. No single strategy can prevent advanced and persistent threats—popularly known as APTs in cybersecurity jargon—from breaching an organization’s cyber defenses.

Policymakers have not sufficiently acknowledged this expensive, practical reality. American companies should not be expected to shoulder the substantial costs of cyberattacks emanating from well-resourced bad actors such as criminal syndicates or nation-states—costs typically absorbed by national governments. Nation-states or their proxies and other sophisticated actors are apparently hacking businesses with impunity—and that has got to stop.

In addition to having policymakers acknowledge cost concerns, the Chamber would welcome working with the administration and Congress on establishing an intelligent and forceful deterrence strategy, utilizing an array of U.S. policy tools, which the United States currently lacks. U.S. policymakers need to focus on pushing back against illicit actors and not on blaming the victims of cybersecurity incidents.<sup>3</sup>

**The Framework Is an Excellent Example of an Effective Public-Private Partnership. Critical Infrastructure Awareness of the Framework Is Strong, and Sector Activities Are Robust and Maturing**

The Chamber believes that the framework—which was released last February—has been a success. The framework represents one of the best examples of public-private partnerships in action. NIST and stakeholders in the public and private sectors should have a great sense of accomplishment. The Chamber, sector-based coordinating councils and associations, companies, and other entities collaborated closely with NIST in developing the framework since the first workshop was held in April 2013.

Critical infrastructure sectors are keenly aware of and supportive of the framework. The Chamber understands that critical infrastructures at “greatest risk” have been identified and engaged by administration officials under the terms of the cyber executive order (EO).<sup>4</sup> Government officials ought to ensure that all resources, particularly the latest cyber threat indicators (CTIs), are available to these enterprises to counter increasing and advanced threats.

Further, important elements of U.S. industry are aware of the framework and are using it or similar risk management tools. Indeed, the Chamber welcomed an assessment from Michael Daniel, White House special assistant to the president and cybersecurity coordinator, who remarked on September 23, 2014, at the Chamber’s third cyber roundtable in Everett, Washington, that industry’s response to the framework has been “phenomenal.”

---

<sup>3</sup> The Chamber submitted comments to the Department of Homeland Security (DHS) on cybersecurity solutions for small and midsize businesses (SMBs) in April 2014.

<sup>4</sup> Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, is available at [www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf](http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf).

A second White House official, Ari Schwartz, senior director for cybersecurity, noted on October 1, 2014, that business support for the framework has “exceeded expectations.” Such recognition is constructive and helps keep the private sector engaged in using the framework and promoting it with business partners.<sup>5</sup>

Much of industry’s favorable reaction is owed in large measure to NIST, which tackled the framework’s development in ways that ought to serve as a model for other agencies and departments. In May 2014, the administration sent the business community a powerful message, saying that the framework should remain collaborative, voluntary, and innovative over the long term.<sup>6</sup> Interestingly, public focus on the framework has created visibility into industry’s long-standing efforts to address cyber risks and threats—constant, dedicated, and mostly silent efforts that preceded the creation of the framework.<sup>7</sup>

Most notable, since the framework’s release, industry has demonstrated its commitment to using it. Many associations are creating resources for their members and holding events across the country and taking other initiatives to promote cybersecurity education and awareness of the framework. Some examples are listed here. Associations are planning and exploring additional activities as well.

- The Alliance of Automobile Manufacturers and the Association of Global Automakers have initiated a process to establish an automobile industry sector information-sharing and analysis center ([Auto-ISAC](#)) to voluntarily collect and share information about existing or potential threats to the cybersecurity of motor vehicle electronics and in-vehicle networks.
- The American Chemistry Council (ACC) is developing sector-specific guidance based on the NIST cyber framework to further enhance and implement the council’s Responsible Care<sup>®</sup> Security [Code](#). ACC’s Chemical Information Technology Center (ChemITC) is also piloting an ISAC for the chemical sector.
- The American Gas Association (AGA) has hosted a series of webinars on control system cybersecurity, is collaborating with small utilities to develop robust cybersecurity programs, and is working with companies to review and enhance their cybersecurity

---

<sup>5</sup> See “At eight-month mark, industry praises framework and eyes next steps,” *Inside Cybersecurity*, October 6, 2014, <http://insidcybersecurity.com/Cyber-Daily-News/Daily-News/at-eight-month-mark-industry-praises-framework-and-eyes-next-steps/menu-id-1075.html>.

<sup>6</sup> The Chamber agrees with Michael Daniel’s May 22 blog, *Assessing Cybersecurity Regulations*, at [www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations](http://www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations). The blog says that business and government “must build equally agile and responsive capabilities not bound by outdated and inflexible rules and procedures.” The Chamber and industry partners especially urge independent agencies and Congress to adhere to the dynamic approach advocated by the administration and embodied in the nonregulatory, public-private framework. See June 11, 2014, multiassociation letter, which is available at [www.uschamber.com/sites/default/files/documents/files/11June14GroupLetterT-YReplytoDanielCyberBlog\\_Final\\_0.pdf](http://www.uschamber.com/sites/default/files/documents/files/11June14GroupLetterT-YReplytoDanielCyberBlog_Final_0.pdf).

<sup>7</sup> The online publication *Inside Cybersecurity* provides an excellent catalog of industry initiatives to implement data- and network-security best practices. See <http://insidcybersecurity.com/Sectors/menu-id-1149.html>.

posture using the Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model ([ONG-C2M2](#)) from the Department of Energy (DOE). Among other activities, AGA has stood up the Downstream Natural Gas Information and Analysis Center ([DNG-ISAC](#)), an ISAC designed to help support the information-sharing interests of downstream natural gas utilities.

- The American Hotel & Lodging Association (AH&LA) has conducted a series of widely attended cyber and data security webinars to assist small, medium, and large hotel and lodging businesses with implementing key information security measures and risk assessments.
- The American Water Works Association (AWWA) has created cybersecurity [guidance and a use-case tool](#) to aid water and wastewater utilities' implementation of the framework. The guidance is cross-referenced to the framework. This tool serves as implementation guidance for the framework in the water and wastewater systems sector.
- Members of the Communications Sector Coordinating Council (CSCC)—made up of broadcasting, cable, wireline, wireless, and satellite segments—have participated in multiple NIST, Department of Homeland Security (DHS), and industry association-sponsored programs, webinars, and panels. The sector is completing a yearlong effort within the Federal Communication Commission's (FCC's) Communications Security Reliability and Interoperability Council ([CSRIC](#)), which involves more than 100 professionals who have worked to adapt the NIST framework to the sector segments and provide guidance to the industry.
- The Electricity Subsector Coordinating Council has worked with DOE to develop sector-specific guidance for using the framework. The guidance leverages existing subsector-specific approaches to cybersecurity, including DOE's *Electricity Subsector Cybersecurity Risk Management Process [Guideline](#)*, the *Electricity Subsector Cybersecurity Capability Maturity [Model](#)*, NIST's *[Guidelines for Smart Grid Cyber Security](#)*, and the North American Electric Reliability Corporation's (NERC's) Critical Infrastructure Protection Cybersecurity [Standards](#).
- The mutual fund industry, represented by the Investment Company Institute (ICI), has added to its committee roster a Chief Information Security Officer Advisory Committee. The committee's mission is to collaborate on cybersecurity issues and information sharing in the financial services industry and provide a cyber threat protection resource for ICI members.
- The Information Technology Industry Council (ITI) visited Korea and Japan in May 2014 and shared with these countries' governments and business leaders the benefits of a public-private partnership-based approach to developing globally workable cybersecurity policies. ITI highlighted the framework as an example of an effective policy developed in this manner, reflecting global standards and industry-driven practices. ITI principals also spoke at a U.S.-European Union (EU) workshop in Brussels in November 2014, comparing U.S. and EU policy approaches with cybersecurity and emphasizing the positive attributes of the framework and its development.

- The National Association of Manufacturers (NAM) has spearheaded the D.A.T.A. (Driving the Agenda for Technology Advancement) Policy [Center](#), providing manufacturers with a forum to understand the latest cybersecurity policy trends, threats, and best practices. The D.A.T.A. Center focuses on working with small and medium-size manufacturers to help them secure their assets.
- Through the American Petroleum Institute (API), the oil and natural gas sector has worked with DOE to complete the Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2). The oil and natural gas sector in 2014 established an Oil and Natural Gas Information Sharing and Analysis Center ([ONG-ISAC](#)) to provide shared intelligence on cyber incidents, threats, vulnerabilities, and responses throughout the industry.
- The Retail Industry Leaders Association (RILA), in partnership with the National Retail Federation (NRF), created the Retail Cyber Intelligence Sharing Center ([R-CISC](#)), featuring information sharing, research, and education and training. This ISAC enables retailers to share threat data among themselves and to receive threat information from government and law enforcement partners.
- The U.S. Chamber of Commerce has launched its national roundtable series, [Improving Today. Protecting Tomorrow](#)<sup>™</sup>, recommending that businesses of all sizes and sectors adopt fundamental Internet security practices.

**Policymakers Need to Focus on Passing Information-Sharing Legislation and Deterring Foreign Attackers. The Chamber’s Cybersecurity Campaign Enters Its Second Year**

The NIST framework is designed to help start a cybersecurity program or improve an existing one. The framework puts cybersecurity into a common language for organizations to better understand their cybersecurity posture, set goals for cybersecurity improvements, monitor their progress, and foster communications with internal and external stakeholders. Looking ahead to 2015, the Chamber’s cybersecurity campaign intends to focus on several areas, including the following:

**Improving information sharing is job No. 1.** The framework would be incomplete without enacting information-sharing legislation that removes legal and regulatory barriers to quickly exchanging data about threats to U.S. companies.

- **Draft Cybersecurity Information Sharing Act (CISA) of 2015**  
On January 27, 35 associations, including the Chamber, urged the Senate to quickly pass a cybersecurity information-sharing bill.<sup>8</sup> The Senate Intelligence committee passed in July 2014 S. 2588, the Cybersecurity Information Sharing Act (CISA) of 2014, a smart and workable bill, which earned broad bipartisan support.

---

<sup>8</sup> The coalition letter is available at [www.uschamber.com/sites/default/files/150127\\_multi-association\\_cyber\\_info-sharing\\_legislation\\_senate.pdf](http://www.uschamber.com/sites/default/files/150127_multi-association_cyber_info-sharing_legislation_senate.pdf).

The committee released in February a new draft bill—CISA 2015—for stakeholder review. Recent cyber incidents underscore the need for legislation to help businesses improve their awareness of cyber threats and enhance their protection and response capabilities.

The Chamber urges Congress to send a bill to the president that gives businesses legal certainty that they have safe harbor against frivolous lawsuits when voluntarily sharing and receiving threat indicators and countermeasures in real time with multiple private and public entities, as well as when monitoring information systems to mitigate cyberattacks.

The legislation also needs to offer protections related to public disclosure, regulatory, and antitrust matters in order to increase the timely exchange of technical CTIs and countermeasures among public and private entities.

The Chamber further believes that legislation needs to safeguard privacy and civil liberties and establish appropriate roles for civilian and intelligence agencies. For example, businesses must remove personal information from CTIs before sharing them. Private entities must share “electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems” with DHS—a *civilian* entity—if they are to be offered protection from liability.

CISA, which is sponsored by Sens. Richard Burr and Dianne Feinstein, reflects practical compromises among many stakeholders on these issues. At the time of this writing, the measure is expected to be marked up the week of March 9. The Chamber looks forward to reviewing the bill following the markup to determine its support for the base measure and any amendments. Industry is likely to strongly support CISA.

- **White House cybersecurity legislative proposal (S. 456, the Cyber Threat Sharing Act of 2015)**

On February 11, S. 456, the Cyber Threat Sharing Act of 2015, was introduced in the Senate by Sen. Tom Carper. It makes sense to refer to S. 456 because it is very similar to the White House’s cybersecurity information-sharing proposal, which was discussed at last week’s House Homeland Security Committee hearing, and released by the administration on January 13.<sup>9</sup>

CISA offers strong protections and flexible avenues for sharing with public and private entities. In contrast, S. 456 would grant liability protections to companies only when sharing CTIs with (1) DHS’ National Cybersecurity and Communications Integration Center (NCCIC)—excluding law enforcement agencies, among others—or with (2) information-sharing and analysis organizations (ISAOs) that have self-certified that they are following information-sharing best practices. (The implications of the ISAOs and the new White House executive order<sup>10</sup> related to promoting cybersecurity information

---

<sup>9</sup> <http://homeland.house.gov/hearing/hearing-administration-s-cybersecurity-legislative-proposal-information-sharing>; [www.whitehouse.gov/omb/legislative\\_letters](http://www.whitehouse.gov/omb/legislative_letters) (see January 13, 2015).

<sup>10</sup> [www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari](http://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari).

sharing, which directs DHS to sponsor an ISAO standards organization to establish a common set of voluntary standards for creating and operating ISAOs, have not been fully assessed by industry.)

These two protected avenues for sharing CTIs are far too narrow and limiting and do not reflect the information-sharing relationships that businesses have built up over time, for instance, with DHS, the departments of Energy and Treasury, and law enforcement agencies.

Unlike CISA, businesses would not be protected under S. 456 when monitoring information systems and sharing or receiving countermeasures. The lack of safeguards in these areas is a fundamental weakness of the White House proposal and S. 456.

Under S. 456, cyber threat data shared with the NCCIC would seemingly be protected from public disclosure and may not be used as evidence in a regulatory action against the entity that shared CTIs, which is welcome. However, S. 456 neither codifies antitrust protections in federal law nor preempts state law. The bill simply references via a sense-of-Congress provision a policy statement that was issued in April 2014 by the Department of Justice and the Federal Trade Commission.<sup>11</sup> While this provision is constructive, antitrust protections need to be written into law to be meaningful to industry.

Similar to CISA, S. 456 includes strong privacy protections. Both bills *narrowly define what CTIs may be shared* among private sector and federal government entities.<sup>12</sup> CISA and S. 456 require that businesses *remove personal information from CTIs* before sharing them. The Chamber urges businesses to share cybersecurity threat data with industry partners and the government. Still, the mandate to scrub personal information would almost certainly sideline smaller businesses, because the provision assumes that businesses would have the technical know-how or the resources to scrub data. To be sure, this outcome is not the intent of the bills' writers, but it is important to note that this is the likely response many businesses would have to such provisions.

And, like CISA, S. 456 would also tightly limit how the federal government could use CTIs that agencies receive. However, unlike CISA, S. 456 would sunset after five years. A sunset provision would almost certainly inhibit businesses' ability to make long-term planning decisions related to risk management and information-sharing investments.

It is necessary to highlight that the Chamber supports CISA. Compared with S. 456, CISA offers a more dynamic approach to sharing cybersecurity threat data among multiple business and government partners, coupled with stronger protections. CISA would go the furthest in helping businesses, including critical infrastructure, defend information systems against cyberattacks. Businesses would likely share and receive

---

<sup>11</sup> [www.justice.gov/opa/pr/justice-department-federal-trade-commission-issue-antitrust-policy-statement-sharing](http://www.justice.gov/opa/pr/justice-department-federal-trade-commission-issue-antitrust-policy-statement-sharing).

<sup>12</sup> CISA 2015 and S. 456 define cyber threat indicators (CTIs) in section 2 of their respective bills.

CTIs and countermeasures and monitor their networks on a broader scale and more confidently because CISA grants stronger liability protections and better policy tools.

**Organizing roundtables with local chambers and growing market solutions.** The Chamber is planning more cyber roundtables in 2015. Last year, the Chamber organized roundtable events with state and local chambers in Chicago, Illinois (May 22); Austin, Texas (July 10); Everett, Washington (September 23); and Phoenix, Arizona (October 8) prior to the Chamber's Third Annual Cybersecurity Summit on October 28.

Leading member sponsors of the campaign were American Express, Dell, and Splunk. Other sponsors were the American Gas Association, Boeing, the Edison Electric Institute, Exelon, HID Global, Microsoft, Oracle, and Pepco Holdings, Inc., and *The Wall Street Journal*.

Each roundtable featured cybersecurity principals from the White House, DHS, NIST, and local FBI and Secret Service officials. The Chamber and its partners urged businesses to adopt fundamental Internet security practices to reduce network and system weaknesses and make the price of successful hacking increasingly steep. The Chamber also urged businesses to improve their cyber risk management processes.

All businesses should understand common online threats that can lead them to become victims of cybercrime. Using the framework and similar risk management tools, such as the Chamber's *Internet Security Essentials for Business 2.0* guidebook,<sup>13</sup> is ultimately about making your business more secure and resilient. The Chamber encourages businesses to report cyber incidents. Perfect online security is unattainable, even for large businesses. Innovative solutions are regularly being brought to market because cyber threats are always changing. Businesses should report cyber incidents and online crime to their FBI or Secret Service field offices.

**Increasing public awareness of the framework.** The Chamber urges policymakers to commit greater resources over the next several years to growing awareness of the framework and risk-based solutions through a national education campaign. A broad-based campaign involving federal, state, and local governments and multiple sectors of the U.S. economy would spur greater awareness of cyber threats and aggregate demand for market-driven cyber solutions.

The Chamber believes that government—particularly independent agencies—should devote their limited time and resources to assisting resource-strapped enterprises, not trying to flex their existing regulatory authority. After all, while businesses are working to detect, prevent, and mitigate cyberattacks originating from sophisticated criminal syndicates or foreign powers, they should not have to worry about regulatory or legal sanctions.

**Engaging law enforcement.** The Chamber plans to continue its close contact with the FBI and the Secret Service to build trusted public-private relationships, which are essential to confirming a crime and beginning criminal investigations. The Chamber encourages businesses to partner with law enforcement before, during, and after a cyber incident. FBI and Secret Service officials have participated in each of the Chamber's roundtables.

---

<sup>13</sup> The booklet is available free for downloading at [www.uschamber.com/issue-brief/internet-security-essentials-business-20](http://www.uschamber.com/issue-brief/internet-security-essentials-business-20).

**Harmonizing cybersecurity regulations.** Information-security requirements should not be cumulative. The Chamber believes it is valuable that agencies and departments are urged under the EO to report to the Office of Management and Budget any critical infrastructure subject to “ineffective, conflicting, or excessively burdensome cybersecurity requirements.” The Chamber urges the administration and Congress to prioritize eliminating burdensome regulations on businesses. One solution could entail giving businesses credit for information security regimes that exist in their respective sectors.<sup>14</sup> It is positive that Michael Daniel, the administration’s lead cyber official, has made harmonizing existing cyber regulations with the framework a priority.

**Raising adversaries’ costs through deterrence.** The Chamber is reviewing actions that businesses and government can take to deter nefarious actors that threaten to empty bank accounts, steal trade secrets, or damage vital infrastructures. While our organization has not formally endorsed the report, the U.S. Department of State’s International Security Advisory Board (ISAB) issued in July draft recommendations regarding cooperation and deterrence in cyberspace.

The ISAB’s recommendations—including cooperating on crime as a first step, exploring global consensus on the rules of the road, enhancing governments’ situational awareness through information sharing, combating IP theft, expanding education and capacity building, promoting attribution and prosecution, and leading by example—are sensible and worthy of further review by cybersecurity stakeholders.<sup>15</sup>

The Chamber believes that the United States needs to coherently shift the costs associated with cyberattacks in ways that are legal, swift, and proportionate relative to the risks and threats. Policymakers need to help the law enforcement community, which is a key asset to the business community but numerically overmatched compared with illicit hackers.<sup>16</sup>

**Making incentives work.** In an April 2013 letter to NIST regarding businesses’ use of the framework and the role of incentives, the Chamber provides its views on extending liability protections related to information-sharing legislation, a safe harbor related to using the framework, SAFETY Act applicability to the framework; eliminating cybersecurity regulations, leveraging federal procurement, and making the research and development (R&D) tax credit permanent.<sup>17</sup>

---

<sup>14</sup> The business community already complies with multiple information security rules. Among the regulatory requirements impacting businesses of all sizes are the Chemical Facilities Anti-Terrorism Standards (CFATS), the Federal Energy Regulatory Commission-North American Reliability Corporation Critical Information Protection (FERC-NERC CIP) standards, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley (SOX) Act. The Securities and Exchange Commission (SEC) issued guidance in October 2011 outlining how and when companies should report hacking incidents and cybersecurity risks. Corporations also comply with many non-U.S. requirements, which add to the regulatory mix.

<sup>15</sup> The ISAB report is available at [www.state.gov/documents/organization/229235.pdf](http://www.state.gov/documents/organization/229235.pdf).

<sup>16</sup> The Chamber argued for a clear cyber deterrence strategy in its December 2013 letter to NIST on the framework. See [http://csrc.nist.gov/cyberframework/framework\\_comments/20131213\\_ann\\_beauchesne\\_uschamber.pdf](http://csrc.nist.gov/cyberframework/framework_comments/20131213_ann_beauchesne_uschamber.pdf).

<sup>17</sup> The letter is available at [www.ntia.doc.gov/files/ntia/29apr13\\_chamber\\_comments.pdf](http://www.ntia.doc.gov/files/ntia/29apr13_chamber_comments.pdf).

The Chamber appreciates that the administration is assessing a mix of incentives that could induce businesses to use the framework.<sup>18</sup> However, in the Chamber’s view, it is imperative that the administration, independent agencies, and lawmakers extend to companies the assurance that the cybersecurity framework and any actions taken in relation to it remain collaborative, flexible, and innovative over the long term. The Chamber believes that the presence of these qualities, or the lack thereof, would be a key determinant to use of the framework by U.S. critical infrastructure as well as businesses generally.

### ***Roadmap for the Future of the Cybersecurity Framework***

In February 2014, NIST released a *Roadmap* to accompany the framework. The *Roadmap* outlines further areas for possible “development, alignment, and collaboration.”<sup>19</sup> The Chamber noted in an October 2014 letter to NIST some key areas that it sees as needing more attention. The Chamber would highlight for the committee the importance of aligning international cybersecurity regimes with the framework.

Many Chamber members operate globally and appreciate that NIST has been actively meeting with foreign governments urging them to embrace the framework. Like NIST, the Chamber believes that efforts to improve the cybersecurity of the public and private sectors should reflect the borderless and interconnected nature of our digital environment.

Standards, guidance, and best practices relevant to cybersecurity are typically industry driven and adopted on a voluntary basis; they are most effective when developed and recognized globally. Such an approach would avoid burdening multinational enterprises with the requirements of multiple, and often conflicting, jurisdictions.<sup>20</sup> The administration should organize opportunities for stakeholders to participate in multinational discussions. The Chamber encourages the federal government to work with international partners and believes that these discussions should be stakeholder driven and occur on a routine basis.

### **Passing an Industry-Supported Information-Sharing Bill Is the Chamber’s Top Cyber Legislative Goal in 2015**

Cyberattacks aimed at U.S. businesses and government entities are being launched from various sources, including sophisticated hackers, organized crime, and state-sponsored groups. These attacks are advancing in scope and complexity. Most policymakers and practitioners appreciate that the intent of legislation is not to spur more information sharing for its own sake. Rather, the goal is to help companies achieve timely and actionable situational awareness to improve the business community’s and the nation’s detection, mitigation, and response capabilities.

---

<sup>18</sup> See [www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework](http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework).

<sup>19</sup> The *Roadmap* is available at [www.nist.gov/cyberframework/upload/roadmap-021214.pdf](http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf).

<sup>20</sup> The Chamber sent a letter in September 2013 to Dr. Andreas Schwab, member of the European Parliament’s Internal Market and Consumer Protection Committee, recommending amendments to the proposed European Union (EU) cybersecurity directive. The Chamber argues that cybersecurity and resilience are best achieved when organizations follow voluntary global standards and industry-driven practices.

Additional positive side effects of enacting cyber information-sharing legislation include strengthening the security of personal information that is maintained on company networks and systems and increasing costs on nefarious actors. The bill would also complement the NIST framework, which many industry associations and companies are embracing and promoting with their business partners. Congressional action on cybersecurity information-sharing legislation cannot come quickly enough.

**WRITTEN STATEMENT OF MARY ELLEN CALLAHAN**  
**Partner and Chair, Privacy and Information Governance Practice, Jenner & Block**  
**Former Chief Privacy Officer, U.S. Department of Homeland Security**

Before the House Committee on Homeland Security, Subcommittee on Cybersecurity,  
Infrastructure Protection, and Security Technologies

*INDUSTRY PERSPECTIVES ON THE PRESIDENT'S CYBERSECURITY INFORMATION SHARING PROPOSAL*

March 4, 2015 Hearing

Chairman Ratcliffe, Ranking Member Richmond, 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 17 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.

Cybersecurity information sharing is vital to protect the private and public sector assets. In order to prepare for disclosing cybersecurity threat indicators to other entities in the cybersecurity ecosystem, however, the information sharing with the government must meet certain standards to address industry interests and needs.

In my testimony, I will address six factors that are crucial to establishing robust, effective private sector information sharing with the government. First and foremost, to encourage and facilitate private sector information sharing, the government must develop and implement legitimate privacy safeguards. Second, clearly established controls must be placed on what the government does with the shared information. Third, those controls must include identifying and empowering a civilian interface with the private sector on information sharing – not just as an intake center, but for all communications related to cybersecurity information sharing. The fourth necessary step is to establish the value proposition for information sharing; information sharing must be at an acceptable cost and provide minimal risk for the participants. Its companion point is to define clear and objective limitations on liability for companies that participate in information sharing – both civilly and criminally. And finally, Congress should expressly provide the Privacy and Civil Liberties Oversight Board with oversight authority over cybersecurity, including information sharing.

**Privacy Safeguards are Essential to Effective Private Sector Information Sharing**

As Apple CEO Tim Cook noted at the Cybersecurity Summit last month, we have to protect our privacy rights or we will all face dire consequences. At the same Summit, President Obama concurred, saying, “When people go online, we shouldn't have to forfeit the basic privacy we're

entitled to as Americans.” However, the *Executive Order on Promoting Private Sector Cybersecurity Information Sharing* does not include a comprehensive privacy and civil liberties framework relating to private sector sharing, instead focusing only on the intra-government sharing, instructing agencies to work with their Senior Agency Officials for Privacy (SAOPs) to ensure that appropriate internal privacy protections are in place.

This decentralized and government-only approach is flawed in two ways. Following the 2013 Executive Order on Improving Cybersecurity, each of the SAOPs for the major agencies prepared their assessments of how they were complying with privacy and civil liberties protections in department to department sharing. The detail and level of analysis by the SAOPs differed greatly. Having a decentralized assessment of privacy impacts, including how to intersect with the private sector, will delay the implementation of adequate privacy protections, and will not instill confidence from the private sector. Furthermore, this decentralized approach does not need to take place under the 2015 Executive Order – because DHS has already has an existing infrastructure in place, and it has been identified as the key department in this private sector information-sharing exercise.

It is unfortunate that the 2015 Executive Order did not elaborate on the necessary privacy and civil liberties protections, particularly with regard to private sector information sharing. Nonetheless, the DHS Privacy Office and Office for Civil Rights and Civil Liberties can lead these inter-agency efforts to address private sector concerns, including with the intersection of Information Sharing and Analysis Organizations (ISAOs).

Without a White House-based privacy policy official, the DHS Chief Privacy Officer frequently serves as *de facto* privacy policy leadership between and among the departments and agencies. As I testified before this Subcommittee in April 2013, DHS has taken multiple steps to integrate cybersecurity and privacy as part of the Department’s cybersecurity mission. 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.”<sup>1</sup>

DHS has been quite transparent about its cybersecurity capabilities. As discussed below, transparency is an important tenet under the FIPPs and an important cornerstone to encourage industry participation. DHS has published several Privacy Impact Assessments (PIAs) detailing pilot programs and information sharing among and between government entities as well as with private companies that have signed Cooperative Research and Development Agreements (CRADAs). This work will assist DHS in establishing deeper relationships with new and existing ISAOs.

The Department already has skilled, dedicated privacy professionals who can help navigate the privacy protections needed for effective information sharing, with multiple cyber privacy professionals on staff. These individuals focus on integrating the FIPPs of purpose specification,

---

<sup>1</sup> The Fair Information Practice Principles as articulated in *National Strategy for Trusted Identities in Cyberspace*, April 2011, available at: [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/NSTICstrategy\\_041511.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf)

data minimization, use limitation, data quality and integrity and security systematically into all 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 personally identifiable information), statements of work, contracts, and international cyber-information sharing agreements. The DHS cyber privacy professionals review all of the CRADAs signed with private companies.

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.<sup>2</sup> 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 ongoing 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.<sup>3</sup> The DHS Privacy Office found the DHS cybersecurity entities generally complied with the privacy requirements in the relevant Privacy Impact Assessments. Specifically, the DHS cybersecurity entities fully complied with collecting information, using information, internal and external sharing with federal agencies and accountability requirements.

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.<sup>4</sup> This investigatory authority may be of interest to the private companies and ISAOs as more private information starts to flow into the government.

The procedures, staffing, accountability and integration into the relationships with private sector entities through CRADAs demonstrate the way in which privacy protections are integrated throughout the DHS cybersecurity program. A framework is in place to address privacy and civil liberties issues for private sector information sharing, and DHS is well positioned to extend those privacy protections to private sector information sharing on a larger scale.

---

<sup>2</sup> See *DHS Privacy Office Annual Report, July 2011-June 2012* at 39-40 for a detailed discussion of Privacy Compliance Reviews.

<sup>3</sup> *Privacy Compliance Review of the EINSTEIN Program*, January 3, 2012, available at: [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_privcomrev\\_nppd\\_ein.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_privcomrev_nppd_ein.pdf).

<sup>4</sup> 6 U.S.C. § 142(b). See *DHS Privacy Office Annual Report, July 2011-June 2012* at 40 for a discussion of the DHS Chief Privacy Officer investigatory authorities.

## **Establish Appropriate Limitations on Information Sharing**

Consistent with the FIPPs and private sector company expectations, there must be clearly defined controls associated with the cybersecurity threat indicators and the related information.

As the DHS portion of the 2013 Executive Order report noted, there are at least three categories of information that companies may provide when sharing cybersecurity threat indicators – information *directly associated* with the cybersecurity threat, information *related* to the cyber threat, and information *incidentally retained* when sharing the threat indicators themselves.<sup>5</sup>

To limit the amount of incidentally retained and related information being shared, companies should implement strict data minimization standards. Frequently, however, it may not be evident upon initial sharing – especially because time may be of the essence -- which information is directly associated with the cybersecurity threat and which information is either incidentally retained or only related to the cyber threat. Therefore, more information than necessary may be shared. As a result, the federal government/DHS should implement a secondary data minimization review and limit any sharing of information only to the information directly associated with the cyber threat.

In certain discussions, there are recommendations to share all cybersecurity threat information – including the related and incidentally retained information – as soon as possible with all government entities. This is ill-advised, for a few reasons. First, this approach does not assist the other entities in identifying the relevant information and requires each agency to re-analyze the information to determine what is relevant and what is not. That is inefficient. Instead, sharing immediately shifts the burden of implementation and analysis to every entity and decentralizes the skill set. If there is a requirement to immediately share, then more information than necessary – and possibly inaccurate information – will be shared throughout the government. For these two reasons, the experts at DHS should first parse the information and apply data minimization principles to allow other agencies to respond quickly to the threat itself, rather than weeding through potentially disparate layers of information. The same principle of double data minimization applies to information sharing between and among companies.

Widespread sharing of related or incidentally retained information will chill information sharing generally. Companies will not want their non-cyber information shared widely, even if there are use limitations. Providing anonymity for producers (especially private companies) – allowing them an environment to share safely without fear of backlash regarding their vulnerabilities – is vital to encourage cooperation. Companies are legitimately concerned that their valuable trade secrets or business sensitive information may be available to the government and their competitors if the non-cyber threat indicators are not minimized.

Even if cyber threat indicators are judiciously shared, use limitations related to the shared information must be in place. In addition to the liability limitations discussed below, the use of

---

<sup>5</sup> *Executive Order 13636 Privacy and Civil Liberties Assessment Report 2014*, available at: <http://www.dhs.gov/sites/default/files/publications/2014-privacy-and-civil-liberties-assessment-report.pdf>

private sector-shared information must be cabined to include only use for cybersecurity threat and response. Relatedly, the federal government (including intelligence agencies) should have limitations on what agencies can retain and for how long with regard to the unique information from companies, rather than the distilled threat indicators.

### **Civilian Control of the Cybersecurity Information Sharing is Crucial to Encourage Private Information Sharing**

Ensuring civilian control of the lifecycle of cybersecurity information from the private sector is critical to comfort private companies before they share cyber threat indicators in volume. Critical infrastructure sectors and companies have reservations that information being shared may not only be used to inform other vulnerable entities, but also would be used for investigations or national security, without any other concomitant benefit. The Executive Order is silent on the issue of civilian control for the lifecycle of the private sector relationship, but that control is crucial to the development of repeatable, consistent information sharing.

Identifying DHS as the private sector interface is vital to placate these concerns. This committee began this process with the legislative establishment of the National Cybersecurity and Communications Integration Center (NCCIC) in 2014 through the National Cybersecurity Protection Act. DHS must continue to be the primary interface with the private sector, and must not just be seen as a pass-through to the intelligence community.

As noted above, DHS has been transparent about its cybersecurity activities, which is imperative to develop credentials and credibility with the private sector. Now that NCCIC has been identified as the leading agency, any information sharing must go through it. As Assistant Secretary Andy Ozment reported to this committee in February, NCCIC received 97,000 incident reports, released 12,000 actionable cyber alerts or warnings and responded to 115 cyber incidents last year. These statistics demonstrate that DHS is maturing. As a civilian agency, it is well positioned to liaise between private companies and the government.

### **Information Sharing Must Not Threaten Companies**

Information sharing must be at an acceptable cost and, therefore, provide minimal risk for the participants. If participants believe they will be targeted by attackers by sharing information, such as configurations, vulnerabilities, or even the fact that they have been targeted, they will not be willing to share information.

DHS has received thorough advice – including from private sector representatives and advocates – as part of its Federal Advisory Committee Act privacy committee, the Data Privacy and Integrity Advisory Committee. The DPIAC issued a significant advisory paper for DHS to consider when implementing information sharing pilots and programs with other entities, including the private sector.<sup>6</sup> The report addresses two important questions in privacy and cybersecurity: “what specific privacy protections should DHS consider when sharing information

---

<sup>6</sup> *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](http://www.dhs.gov/sites/default/files/publications/privacy/DPIAC/dpiac_cyberpilots_10_29_2012.pdf).*

from a cybersecurity pilot project with other agencies?” and “what privacy considerations should DHS include in evaluating the effectiveness of cybersecurity pilots?” This type of advice helps DHS design systems to avoid antagonizing companies and ISAOs and comfort them they will not somehow be punished for participating.

### **Limitations on Liability Must Be Clearly Defined**

The issue of liability limitations has been discussed at length during the pendency of the cybersecurity legislation. It obviously is an important issue for companies, and it needs to be resolved appropriately in order to encourage information sharing. With that said, having clearly defined limitations may help companies even more than having a “notwithstanding any other law” blanket exception.

The liability limitation must address at least two aspects directly. First, the shared information cannot be shared with other agencies and then used in a civil or criminal enforcement action against the sharing company. That is crucial. Furthermore, the shared information should not be used in civil or criminal enforcement actions against a third party who is not the cyber attacker – namely, if shared information contains damning information either about the sharing company or a third party company, the government’s awareness of that information cannot lead to enforcement.

Furthermore, companies and ISAOs need to be comforted that the information they share will be appropriately protected. The DHS transparency on its systems will hopefully ameliorate that concern.

The antitrust concerns raised in earlier Congresses have waned in light of the Joint Department of Justice/Federal Trade Commission Statement *Antitrust Policy Statement on Sharing of Cybersecurity Information*.<sup>7</sup> Nonetheless, more clarity, particularly *vis a vis* inter-company sharing, will induce more information sharing.

### **Privacy and Civil Liberties Oversight Board Should Be Granted Oversight Authority over Cybersecurity Information Sharing**

The Privacy and Civil Liberties Oversight Board (PCLOB) serves an important oversight function on intelligence and national security activities related to terrorism. The PCLOB’s authority should be expanded to include oversight on cybersecurity activities, including information sharing with and from the private sector. This addition will further bolster the FIPPs throughout the cyber information sharing lifecycle, and will provide additional oversight capacity over the collection, use, sharing and retention of private sector information.

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

\*\*\*

---

<sup>7</sup> <http://www.justice.gov/atr/public/guidelines/305027.pdf>.



**Financial Services Sector Coordinating Council**  
for Critical Infrastructure Protection and Homeland Security

Testimony of

**Gregory T. Garcia**

*On Behalf of the*

**Financial Services Sector Coordinating Council**

*On*

Industry Perspectives on the President's  
Cybersecurity Information Sharing Proposal

*Before the*

United States House of Representatives  
Committee on Homeland Security  
Subcommittee on Cybersecurity, Infrastructure Protection, and  
Security Technologies

March 4, 2015

Chairman Ratcliffe, Ranking Member Richmond, and members of the Subcommittee, thank you for this opportunity to address the Subcommittee about the President's information sharing executive order.

My name is Gregory T. Garcia. I am Executive Director of the Financial Services Sector Coordinating Council (FSSCC), which was established in 2002 and involves 65 of the largest financial services providers and industry associations representing clearinghouses, commercial banks, credit card networks and credit rating agencies, exchanges/electronic communication networks, financial advisory services, insurance companies, financial utilities, government-sponsored enterprises, investment banks, merchants, retail banks, and electronic payment firms.

### **FSSCC MISSION**

The mission of the FSSCC is to strengthen the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure by proactively identifying threats and promoting protection, driving preparedness, collaborating with the federal government, and coordinating crisis response for the benefit of the financial services sector, consumers and the nation's economic security. During the past decade, this strategic partnership has continued to grow, in terms of both the size and commitment of its membership and the breadth of issues it addresses. Members volunteer their time and resources to FSSCC with a sense of responsibility to the broader sector, financial consumers and the nation.

In simplest terms, members of the FSSCC assess security and resiliency trends and policy developments affecting our critical financial infrastructure, and coordinate among ourselves and with our partners to develop a consolidated point of view and coherent strategy for dealing with those issues.

Accordingly, our sector's primary objectives are to:

1. Implement and maintain structured routines for sharing timely and actionable information related to cyber and physical threats and vulnerabilities among firms, across sectors of industry, and between the private sector and government.
2. Improve risk management capabilities and the security posture of firms across the financial sector and the service providers they rely on by encouraging the development and use of common approaches and best practices.
3. Collaborate with homeland security, law enforcement and intelligence communities, financial regulatory authorities, other sectors of industry, and international partners to respond to and recover from significant incidents.
4. Discuss policy and regulatory initiatives that advance infrastructure resiliency and security priorities through robust coordination between government and industry.

To achieve these objectives we partner with the Department of Treasury, DHS, law enforcement, and financial regulatory agencies forming our Government Coordinating Council counterpart – called the Financial and Banking Information Infrastructure Committee (FBIIIC).

Rolling up into those broad objectives are numerous initiatives undertaken collaboratively within this public-private partnership, including committee-organized workstreams to, for example:

- improve Information sharing content and procedures between government and the sector
- conduct joint exercises to test our resiliency and information sharing procedures under differing scenarios
- prioritize critical infrastructure protection research and development funding needs
- engage with other critical sectors and international partners to better understand and leverage our interdependencies
- advocate broad adoption of the NIST Cybersecurity Framework, including among small and mid-sized financial institutions across the country
- develop best practices guidance for operational risk issues involving third party risk, supply chain, and cyber insurance strategies.

We have learned over the years that a foundational element of any strong risk management strategy for cyber and physical protection involves participation in communities of trust that share information related to threats, vulnerabilities, and incidents affecting those communities. That foundation is based on the simple concepts of strength in numbers, the neighborhood watch, and shared situational awareness.

To achieve this goal, public and private sector partners exchange data and contextual information about specific incidents and longer term trends and developments. Sharing this information helps to prevent incidents from occurring and to reduce the risk of a successful incident at one firm later impacting another. These efforts increasingly focus on including smaller firms and include international partners.

Financial sector stakeholders participate in information sharing programs operated by the Department of Homeland Security. For example, the financial sector and Treasury Department maintain a presence within the National Cybersecurity and Communications Integration Center (NCCIC), which serves as a hub for sharing information related to cybersecurity and communications incidents across sectors, among other roles and responsibilities. The sector also works closely with the National Infrastructure Coordinating Center (NICC), which is the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the federal government.

The financial sector benefits greatly from its close information sharing relationship with law enforcement partners, including the Federal Bureau of Investigations and the United States Secret Service.

### **FS-ISAC INFORMATION SHARING PROGRAMS AND OPERATIONS**

For the financial sector, the primary community of trust for critical financial infrastructure protection is the Financial Services Information Sharing and Analysis Center, or FS-ISAC, which is the operational heartbeat of the FSSCC strategic body.

The FS-ISAC was formed in 1999 in response to the 1998 Presidential Decision Directive 63 (PDD 63), which called for the public and private sectors to work together to address cyber threats to the nation's critical infrastructures. After 9/11, and in response to Homeland Security Presidential Directive 7 (and its 2013 successor, Presidential Policy Directive 21) and the Homeland Security Act, the FS-ISAC expanded its role to encompass physical threats to our sector.

The FS-ISAC is a 501(c)6 nonprofit organization and is funded entirely by its member firms and sponsors. In 2004, there were only 68 members of the FS-ISAC, mostly larger financial services firms. Since that time the membership has expanded to more than 5000 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, data security payments processors, and 24 trade associations representing virtually all of the U.S. financial services sector.

Since its founding, the FS-ISAC's operations and culture of trusted collaboration have evolved into what we believe is a successful model for how other industry sectors can organize themselves around this security imperative. The overall objective of the FS-ISAC is to protect the financial services sector against cyber and physical threats and risk. It acts as a trusted third party that provides anonymity to allow members to share threat, vulnerability and incident information in a non-attributable and trusted manner. The FS-ISAC provides a formal structure for valuable and actionable information to be shared amongst members, the sector, and its industry and government partners, which ultimately benefits the nation. FS-ISAC information sharing activities include:

- delivery of timely, relevant and actionable cyber and physical email alerts from various sources distributed through the FS-ISAC Security Operations Center (SOC);
- an anonymous online submission capability to facilitate member sharing of threat, vulnerability and incident information in a non-attributable and trusted manner;
- operation of email listservs supporting attributable information exchange by various special interest groups including the Financial Services Sector Coordinating Council (FSSCC), the FS-ISAC Threat Intelligence Committee, threat intelligence sharing open to

the membership, the Payment Processors Information Sharing Council (PPISC), the Clearing House and Exchange Forum (CHEF), the Business Resilience Committee, and the Payments Risk Council;

- anonymous surveys that allow members to request information regarding security best practices at other organizations;
- bi-weekly threat information sharing calls for members and invited security/risk experts to discuss the latest threats, vulnerabilities and incidents affecting the sector;
- emergency threat or incident notifications to all members using the Critical Infrastructure Notification System (CINS);
- emergency conference calls to share information with the membership and solicit input and collaboration;
- engagement with private security companies to identify threat information of relevance to the membership and the sector;
- participation in various cyber exercises such as those conducted by DHS (Cyber Storm I, II, and III) and support for FSSCC exercises such as CyberFIRE and Quantum Dawn
- development of risk mitigation best practices, threat viewpoints and toolkits, and preparation of cyber security briefings and white papers;
- administration of Subject Matter Expert (SME) committees including the Threat Intelligence Committee and Business Resilience Committee, which: provide in-depth analyses of risks to the sector, conduct technical, business and operational impact assessments; determine the sector's cyber and physical threat level; and, recommend mitigation and remediation strategies and tactics;
- special projects to address specific risk issues such as the Account Takeover Task Force
- document repositories for members to share information and documentation with other members;
- development and testing of crisis management procedures for the sector in collaboration with the FSSCC and other industry bodies;
- semi-annual member meetings and conferences; and

- online webinar presentations and regional outreach programs to educate organizations, including small to medium sized regional financial services firms, on threats, risks and best practices.

### **FS-ISAC PARTNERSHIPS**

The FS-ISAC works closely with various government agencies including the U.S. Department of Treasury, Department of Homeland Security (DHS), Federal Reserve, Federal Financial Institutions Examination Council (FFIEC) regulatory agencies, United States Secret Service, Federal Bureau of Investigation (FBI), the intelligence community, and state and local governments.

In partnership with DHS, FS-ISAC two years ago became the third ISAC to participate in the National Cybersecurity and Communications Integration Center (NCCIC) watch floor. FS-ISAC representatives, cleared at the Top Secret / Sensitive Compartmented Information (TS/SCI) level, attend the daily briefs and other NCCIC meetings to share Data information on threats, vulnerabilities, incidents, and potential or known impacts to the financial services sector. Our presence on the NCCIC floor has enhanced situational awareness and information sharing between the financial services sector and the government, and there are numerous examples of success to illustrate this.

As part of this partnership, the FS-ISAC set up an email listserv with U.S. CERT where actionable incident, threat and vulnerability information is shared in near real-time. This listserv allows FS-ISAC members to share directly with U.S. CERT and further facilitates the information sharing that is already occurring between FS-ISAC members and with the NCCIC watch floor or with other government organizations.

In addition, FS-ISAC representatives sit on the Cyber Unified Coordination Group (Cyber UCG). This group was set up under authority of the National Cyber Incident Response Plan (NCIRP) and has been actively engaged in incident response. Cyber UCG's handling and communications with various sectors following the distributed denial of service (DDOS) attacks on the financial sector in late 2012 and early 2013 is one example of how this group is effective in facilitating relevant and actionable information sharing.

Consistent with the directives of Presidential Policy Directive 21 and Executive Order 13636 of 2014, the Treasury established the Cyber Intelligence Group (CIG) as part of the Office of Critical Infrastructure Protection and Compliance Policy. The CIG was established in response to a need identified by the financial sector for the government to have a focal point for sharing cyber threat-related information with the sector. The CIG identifies and analyzes all-source intelligence on cyber threats to the financial sector; shares timely, actionable information that alerts the sector to threats and enables firms' prevention and mitigation efforts; and solicits feedback and information requirements from the sector.

Finally, it should be noted that the FS-ISAC and FSSCC have worked closely with its government partners to obtain security clearances for key financial services sector personnel. These clearances have been used to brief the sector on new information security threats and have provided useful information for the sector to implement effective risk controls to combat these threats.

In addition, several membership subgroups meet regularly with their own circles of trust to share information, including: the Insurance Risk Council (IRC); the Community Institution Council (CIC) with hundreds of members from community banks and credit unions; and the Community Institution Toolkit Working Group with a mission to develop a framework and series of best practices to protect community institutions. This includes a mentoring program to assist community institutions just getting started with an IT security staff.

The FS-ISAC also works very closely with the other critical infrastructure sectors on an ISAC to ISAC basis as well as through the National Council of ISACs. Information about threats, incidents and best practices is shared daily among the ISACs via ISAC analyst calls, and a cross-sector information sharing platform. The ISACs also come together during a crisis to coordinate information and mitigations as applicable.

### **AUTOMATED THREAT INFORMATION SHARING**

The sector continues to make significant progress toward increasing the speed and reliability of its information sharing efforts through expanded use of DHS-funded open specifications, including Structured Threat Information eXchange (STIX™) and Trusted Automated eXchange of Indicator Information (TAXII™).

Late last year, the financial sector announced a new automated threat capability it created called “Soltra Edge”, which is the result of a joint venture of the FS-ISAC and the Depository Trust and Clearing Corporation. This capability addresses a fundamental challenge in our information sharing environment: typically the time associated with chasing down any specific threat indicator is substantial. The challenge has been to help our industry increase the speed, scale and accuracy of information sharing and accelerate time to resolution.

The Soltra Edge capability developed by the sector removes a huge burden of work for both large and small financial organizations, including those that rely on third parties for monitoring and incident response. It is designed for use by many parts of the critical infrastructure ecosystem, including the financial services sector, the healthcare sector, the energy sectors, transportation sectors, other ISACs, national and regional CERTs (Computer Emergency Response Teams) and vendors and services providers that serve these sectors.

Key goals of Soltra-Edge are to:

- Deliver an industry-created utility to automate threat intelligence sharing

- Reduce response time from days/weeks/months to seconds/minutes
- Deliver 10 times reduction in effort and cost to respond
- Operate on the tenets of at-cost model and open standards (STIX, TAXII)
- Leverage DTCC scalability; FS-ISAC community & best practices
- Provide a platform that can be extended to all sizes of financial services firms, other ISACs and industries
- Enable integration with vendor solutions (firewalls, intrusion detection, anti-virus, threat intelligence, etc.)

With these advancements, one organization's incident becomes everyone's defense at machine speed. We expect this automated solution to be a 'go to' resource to speed incident response across thousands of organizations in many countries within the next few years.

### **EXERCISES**

The sector regularly tests its resilience through exercises to identify gaps and exercise processes related to information sharing. Efforts such as the annual "Cyber Attack against Payment Processes (CAPP)", "Quantum Dawn" and public/private exercises provide essential insight into our ability individually and collaboratively to respond to various attack scenarios.

In carrying out this information sharing partnership, the financial sector and government partners are committed to ensuring that individual privacy and civil liberties protections are incorporated into all activities, to include technical analysis, information sharing on threats, and incident response efforts.

### **THE PRESIDENT'S EXECUTIVE ORDER ON PROMOTING PRIVATE SECTOR CYBERSECURITY INFORMATION SHARING**

As discussed above, the Financial Services Sector Coordinating Council (FSSCC) considers strong collaboration and information sharing within the sector and with government to be a critical element of cybersecurity risk management.

Thus, in alignment with the FS-ISAC's statement for the record by Denise Anderson, vice president of the FS-ISAC and Chair of the National Council of ISACs, we applaud this Administration's efforts to improve our cybersecurity information sharing environment so that we can better anticipate, protect against and respond to cyber threats. The Administration's executive action is a positive step toward increasing the volume and quality of actionable and timely cybersecurity information.

With key federal support from the Treasury Department as our Sector Specific Agency, law enforcement and the Department of Homeland Security (DHS), our network defenders are better able to prepare for

cyber threats when there is a consistent, reliable and sustainable flow of actionable cybersecurity information and analysis, at both a classified and unclassified level.

We are making some progress toward this goal, but it has become increasingly necessary for appropriately-cleared representatives of critical sectors such as financial services to have access, and provide contributions, to classified information that enables analysts and operators to take timely action to defend essential systems. Accordingly, the executive order's enhancement of DHS's role in accelerating the security clearance process for critical sector owners and operators is a clear indication of the Administration's support for this public-private partnership.

In considering enhancements to this model, agility and innovation are essential for the operational resilience of critical sector functions. In this spirit, we support the creation of Information Sharing and Analysis Organizations (ISAOs) as a mechanism for all sectors, regions and other stakeholder groups to share cybersecurity information and coordinate analysis and response.

While ISACs must retain their status as the government's primary critical infrastructure partners given their mandate for broad sectoral representation, the development of ISAOs should be facilitated for stakeholder groups that require a collaborative cyber and physical threat information sharing capability that builds on the strong foundation laid by the ISACs.

As the ISAO standards development process unfolds, the FSSCC believes certain principles must be upheld for structuring both the ISAOs themselves and the government's interaction with them:

- Sharing of sensitive security information within and among communities of trust is successful when operational standards of practice establish clear and enforced information handling rules.
- Information sharing is not a competitive sport: while competition in innovation can improve technical capabilities, operational standards should incentivize federated information sharing. Threat and vulnerability intelligence needs to be fused across trust communities, not diffused or siloed.
- Government internal processes for collecting, analyzing and packaging CIP intelligence for ISAC/ISAO consumption must be streamlined and transparent to maximize timeliness, accuracy and relevance of actionable shared information. Indeed, Section 4 of EO 13636 directs the government to improve its dissemination of cyber threat intelligence to the private sector, enabling entities to protect their networks. Full implementation of this directive is necessary to achieve the objectives of the President's information sharing executive order.
- To manage scarce resources, government information sharing mechanisms such as the National Cyber and Communications Integration Center (NCCIC) and the Treasury Department's Cyber Intelligence Group (CIG) should prioritize engagements with ISACs and ISAOs according to transparently established impact criteria, such as government capacity to effectively serve CIP constituents in steady-state and surge mode, the reach those CIP stakeholders have into their sectors, and the effectiveness of their capabilities.

It is also important that the process to develop the ISAO standards is collaborative, open, and transparent. The process managed by the National Institute of Standards and Technology (NIST) during the development of the NIST Cybersecurity Framework is an excellent example of the appropriate leveraging of private sector input, knowledge and experience to develop guidance that will primarily impact non-governmental entities. We encourage DHS, as the implementing authority of the

president's EO, to emulate the engagement model that NIST used to create and adopt their Cybersecurity Framework. The process worked.

Finally, for DHS to be successful implementing this EO and its many cyber security risk management and partnership authorities, it must be sufficiently resourced with the best analytical and technical capabilities, with a cadre of highly qualified cybersecurity leaders and analytical teams to conduct its mission. There must be a concerted effort to recruit, retain and maintain a world class workforce that is able to assess cyber threats globally and help the private sector reduce risk to this nation.

The FSSCC believes that, with the application of the principles discussed in this statement, the creation of ISAOs and their partnership agreements with DHS have the potential to complement the ISAC foundation and measurably improve cyber risk reduction for critical infrastructure and the national economy.

On the subject of legislation, Mr. Chairman, passing cyber threat information sharing legislation that encourages more information sharing between the private sector and government and within the private sector, with fewer concerns about liability, will have a positive operational impact on the security of the nation's networks. This sector-wide position is articulated in detail in recent letters from leading financial services trade associations.

Mr. Chairman and Members of the Committee, this concludes my testimony.

# Sharing Information about Threats is not a Cybersecurity Panacea

Martin C. Libicki

RAND Office of External Affairs

CT-425

March 2015

Testimony presented before the House Homeland Security Committee, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies on March 4, 2015

This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. RAND® is a registered trademark.



Published 2015 by the RAND Corporation  
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138  
1200 South Hayes Street, Arlington, VA 22202-5050  
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665  
RAND URL: <http://www.rand.org/>  
To order RAND documents or to obtain additional information, contact  
Distribution Services: Telephone: (310) 451-7002;  
Email: [order@rand.org](mailto:order@rand.org)

**Martin C. Libicki<sup>1</sup>**  
**The RAND Corporation**

***Sharing Information about Threats is not a Cybersecurity Panacea<sup>2</sup>***

**Before the Committee on Homeland Security  
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies  
House of Representatives**

**March 4, 2015**

Good morning, Chairman Ratcliffe, Ranking Member Richmond, and distinguished members of the subcommittee. I thank you for the opportunity to testify today about the President's cybersecurity information-sharing proposal.

The President's initiatives to improve cybersecurity through information-sharing are laudable. Information-sharing can and should be an important element in efforts to ensure that defenders learn from each other faster than attackers learn from each other. The fact that attackers *do* learn from each other is something that we know from research that RAND conducted for a report released last year on cybercrime markets (*Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*).

People have been calling for greater information-sharing for almost 20 years, dating back to the formation of Information Sharing and Analysis Centers (ISACs) in the late 1990s and continuing through the recent reformulation of ISACs into Information Sharing and Analysis Organizations (ISAOs). Although more information *is* being shared, the President's initiatives are prompted by the perception that information-sharing is not advancing fast enough. Those asked to share gain little directly from sharing and believe they face financial, reputational, and legal risks in doing so. As a result, legislation has been repeatedly introduced to facilitate the increased exchange of information—notably, I would argue, *threat* information. Without going into a detailed assessment of the privacy implications of such legislation, apart from noting that concerns *have* been raised, its purposes are nevertheless sound and its passage can help improve cybersecurity.

Two concerns, however, merit note. One is that the current proposals do not address, and may even exacerbate, the differences between the cybersecurity enjoyed by small- and medium-sized

---

<sup>1</sup> The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

<sup>2</sup> This testimony is available for free download at <http://www.rand.org/pubs/testimonies/CT425.html>.

enterprises on the one hand and that enjoyed by large enterprises on the other: a cybersecurity divide. The second concern is that the current legislative proposals represent an enormous amount of political energy dedicated to what is actually a narrowly focused point solution to the problem of cybersecurity when a much broader approach is required. Consider each concern in turn.

The cybersecurity divide exists roughly at the boundary between those organizations that are large enough to afford their own chief information security officer (CISO) and those that cannot. As a very rough estimate, though this varies by sector, organizations with more than one thousand employees can afford to hire a CISO, and those that are smaller cannot. Organizations that cannot afford to employ a CISO can usually offer only generalized cybersecurity training for their employees (if they do so at all); must rely on commodity hardware and software, often deployed with default settings; make do with commercial network offerings such as routers; and use off-the-shelf firewall tools. Organizations that can afford to employ a CISO can offer and customize specialized training, can afford to optimize their hardware and software for cybersecurity, can purchase sophisticated cybersecurity tools, can hire information security analysts, and contract with third parties for additional cybersecurity services. Fortunately, cloud offerings can be and are tailored for organizations of all sizes, but this only represents a partial approach to cybersecurity and may introduce a few additional security problems of their own.

ISAOs, laudable as they may be, are oriented toward organizations that can afford their membership fees; at \$10,000 a year, most small- and medium-sized organizations are priced out of that market. Consider the likelihood that these ISAO's become the primary—or worse, exclusive—conduit for information-sharing between the government and private organizations. If so—and in the absence of other mechanisms to share information with the broader public—the smaller organizations are going to be left out. Whatever advantage they reap from information-sharing rests on the hope that the existence of ISAOs as conduits for shared information does not detract from paths more suited to smaller enterprises.

The risks of exacerbating the cybersecurity divide are related to the problem of an overly narrow focus for information-sharing associated with pending legislation.

Several weeks ago, during the Cybersecurity Summit, President Obama said, “There’s only one way to defend America from cyberthreats, and that’s government and industry working together [and] sharing appropriate information.” However, cybersecurity is not that elementary; there is no one unique way. Furthermore, the associated Executive Order calls for “fostering the development and adoption of automated mechanisms for the sharing of information.” That being

so, not only is information-sharing not the “only one way” to improve cybersecurity, but the model proposed for information-sharing is also not the “only one way” to share information.

To explain why requires stepping back to take a broader look at information-sharing. Among the many types of information-sharing, three merit note.

First is the process by which software vulnerabilities are brought to the attention of those who make and maintain software. A large percentage of all networks—particularly the more diligently defended ones—are penetrated because their software contains vulnerabilities that have not been fixed, notably because the vendors have not discovered them. These are “zero-day vulnerabilities”; they permit “zero-day exploits.” Software vulnerabilities in Java, Acrobat, Flash, and Microsoft Office products are commonly exploited to allow attackers to enter computer networks and systems (which is why users are warned not to click on suspect websites or open suspicious attachments). A large and growing community of researchers and white-hat hackers are busy finding these vulnerabilities and reporting them to vendors. A related community examines actual cyberattacks to determine which vulnerabilities were exploited in order to serve the same end of fixing them. A world with fewer software vulnerabilities would be a safer world (although patches do no good until installed). Occasionally, software vendors confronted with a number of similar vulnerability reports about their products may find correlated architectural weaknesses in their offerings and make more fundamental changes. The federal government can do more to encourage and accelerate the process of finding software vulnerabilities with modest amounts of funding and without passing new legislation.

Second is the use of information-sharing to improve cybersecurity *practice*. The collection and analysis of cyberattacks, both those that succeed and those that may be termed near misses, can shed light on what organizations could have done differently to have prevented or at least mitigated the effects of such attacks. Such analysis can provide evidence-based assessments of the cost-effectiveness of alternative cybersecurity tools and techniques. Such an activity is already informally carried out to some extent at the worker level, especially among the information security community and disseminated through professional interaction. This should continue to be encouraged, and should trickle up to the C-Suite and managers. Such activity can lead to insights that are scientifically validated (or refuted), which then become part of the cybersecurity canon, to be spread through the literature and other formal and informal exchanges within the information technology community, as well as taught in the various schoolhouses. The government can aid this process by empowering organizations such as the National Institute of Standards and Technology (NIST) and funding the various Advanced Research Project Agencies (ARPAs) and the National Science Foundation (NSF) to build a systematic body of knowledge.

These first two types of information-sharing do not exacerbate the cybersecurity divide. The first should result in better software, which benefits everyone. The second should result in better cybersecurity practices, which also should benefit everyone, particularly those organizations that have at least one person who can think systematically about cybersecurity.

This now leaves the third type of information-sharing, one that is specific to the characterization of threats and the impetus behind the legislation. It calls for organizations to report attacks and provide relevant details of these attacks, such as malware samples, attacker *modus operandi*, IP addresses, attack vectors, induced anomalies, social engineering methods, etc. These instances, in turn, are used to create a profile of specific threat actors and infer signatures of their activities, which, in turn, would be circulated to other organizations so that they can better prepare themselves, notably by putting such signatures into their intrusion prevention/detection systems. The appendix of the 2013 Mandiant report (*APT1: Exposing One of China's Cyber Espionage Units*), for instance, was stuffed with many signatures that could be used by potential victims of APT1 (their name for a specific hacker group supported by China's Peoples Liberation Army) to recognize signs of threat activity infection. Although such signatures could, and in many cases, would also be supplemented by intelligence collection, the classified nature of such additional material limits the number and type of machines on which they could reside.

The usefulness of threat-based information-sharing rests on four assumptions about the nature of the threat itself. Such assumptions would have to be largely or totally true before the value of establishing an information-sharing apparatus can justify the effort to operate it, persuade organizations to contribute to it, and offset the residual risks to privacy that such information transfer may entail.

*The first assumption* is that a sufficient share of all serious attacks comes from specific black-hat hacker groups and that each carry out enough attacks over a period of time so that their *modus operandi* can be characterized. Trivially, if every black-hat hacker organization carried out just one attack, signatures derived from that one attack would inform no further attacks. In practice, each group must carry out enough attacks so those that are discovered can inform those that take place later on. Furthermore, for such signatures to be useful, there has to be time for the attack to be detected so that the signatures can be collected, shared, and inserted into the defensive systems of potential future victims while they are still useful. If all the attacks were bunched together in a short period, the information gathered from such attacks will not be gathered in time to be useful.

*The second assumption* is that each attacker group generates a consistent set of signatures that recur in multiple attacks (and that can be used reliably by defenders to distinguish their attacks from benign activity). To wit, hacker signatures have to resemble fingerprints. The APT1 group's attacks did have such characteristics (similarly, those that attacked Sony Pictures Entertainment in late 2014 used the same IP addresses as those who attacked South Korean banks and media firms in 2013). However, the possibilities of polymorphic malware (variations in the appearance of exploits) and fast-flux DNS (to permit shifting IP addresses) suggest that hackers have options for varying their signatures.

*The third assumption* is that these signatures are detectable by organizations interested in sharing. The average attacks by sophisticated and advanced threats remain undetected for a year—and those are only the ones that have been discovered. Most such attacks are discovered not by their victims but by third parties and, for the most part, only because the information taken from several victims is funneled through the same intermediate servers used to hold the exfiltrated data. If these servers are discovered, evidence from attacks on multiple victims can be picked up at the same time. Attackers who are sensitive to being caught can explore alternative ways to route the data they bring home.

*The fourth assumption* is that such signatures will not evolve (enough) over time—even if information-sharing became so widespread that the failure to evolve would make it too hard for hacker groups to penetrate and compromise networks. Although Mandiant's publication of APT1 activities slowed the group's activities, it only took a few months before they were back in business using a new set of exploits and attack vectors, with brand new signatures that had to be inferred.

An analogy may be drawn to the anti-virus industry. The major players—Symantec, McAfee, Kaspersky, and Microsoft—run very large information-gathering networks fed by inputs from customers as well as sensors that they have placed throughout the Internet. But the anti-virus model has lost most of its viability over the past five years in the face of ever-shifting signatures and the practice of attackers testing malware against anti-virus suites before releasing them into the wild. Although threat-centric information-sharing deals with a broader range of indicators than anti-virus companies do, the same dynamic by which expensively constructed measures beget relatively low-cost countermeasures argues against being terribly optimistic about the benefits from pushing a threat-centric information-sharing model.

This is not to say that threat-centric information-sharing is useless. Not every black-hat hacker group will be conscientious about altering its modus operandi, and there may be features of their

signatures that are not obvious to themselves (and hence would likely persist for later detection). Forcing such groups to cluster their attacks or to use multiple attack vectors, including obfuscation techniques and grouping methods, resulting in new or altered signatures over time, means more work for them. Some attackers will drop out; others may not be able to attack as many organizations in a given period. So, the effort to gather signatures would not be completely wasted. Furthermore, even if threat-centric information-sharing does not work, the efforts that organizations would have to make to understand what is going on in their networks in order to share information effectively would, as a side-benefit, also help them protect themselves absent any information-sharing whatsoever.

Unfortunately, these recent efforts to promote a particular kind of information-sharing have achieved the status of a panacea. They are absorbing a disproportional share of the legislative and elite media energy on the topic of cybersecurity. Many otherwise serious people assert that information-sharing could have prevented many headline assaults on important networks. Yet, if one works through such attacks to understand if there were precedents that could have given us threat signatures, one often finds no good basis for such a belief. Quelling the nation's cybersecurity problems is a complex, multi-faceted endeavor not subject to a silver bullet.

In sum, there is nothing wrong with information-sharing. It should be encouraged. The President's proposal may well do so—in which case it deserves our support. But there is something wrong with assuming that it solves most, much less all, of the cybersecurity problem. It only addresses one facet of a very complex space. It is therefore highly questionable whether efforts to achieve information-sharing deserve the political energy that they are currently taking up.

I appreciate the opportunity to discuss this important topic, and I look forward to your questions.