Statement of the U.S. Chamber of Commerce

ON: Oversight of the Cybersecurity Act of 2015

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

DATE: June 15, 2015

1615 H Street NW | Washington, D.C. | 20062

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 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.

Matthew J. Eggers
Executive Director, Cybersecurity Policy, U.S. Chamber of Commerce
House Homeland Security Committee
Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee
Oversight of the Cybersecurity Act of 2015
June 15, 2016

Good morning, Chairman Ratcliffe, Ranking Member Richmond, and other distinguished members of the Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee (subcommittee). My name is Matthew Eggers, and I am the executive director of cybersecurity policy with 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 regarding oversight of the Cybersecurity Act of 2015.

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'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.

The Chamber applauds the House Homeland Security Committee (committee) and its staff members for their dedication to getting cybersecurity information-sharing legislation enacted. Recent cyber incidents in the public and private sectors underscore the need for legislation to help businesses improve their awareness of cyber threats and to enhance their protection and response capabilities in collaboration with government entities. Cyberattacks aimed at businesses and government bodies are increasingly being launched from sophisticated hackers, organized crime, and state-sponsored groups. These attacks are advancing in scope and complexity. Industry and government have a mutual interest in bolstering the economic security of the U.S. business community.

CYBERSECURITY INFORMATION SHARING ACT OF 2015 (CISA): THE BASICS

I will largely confine my written statement to the Cybersecurity Information Sharing Act of 2015 (CISA), which is title I of the Cybersecurity Act of 2015.[1] President Obama signed this legislation into law in December 2015. The House passed two cybersecurity information-sharing bills in April 2015 with robust majorities from both parties and with broad industry backing. Indeed, the House's action prodded the full Senate to take up cybersecurity information-sharing legislation in the fall.

Passing cybersecurity information-sharing legislation was the top cyber policy priority of the Chamber. We led the Protecting America's Cyber Networks Coalition (the coalition), a partnership of more than 50 leading business associations representing nearly every sector of the U.S. economy. It took a dedicated team working with Capitol Hill and the administration to get CISA done.

CISA establishes a voluntary information-sharing program, intended to strengthen businesses' protection and resilience against cyberattacks. The law gives businesses legal

certainty that they have safe harbor against frivolous lawsuits when freely sharing and receiving cyber threat indicators (CTIs) and defensive measures (DMs) in real time and taking actions to mitigate cyberattacks. CISA also offers protections related to public disclosure, regulatory, and antitrust matters in order to increase the timely exchange of information among public and private entities.

The law safeguards individuals' privacy and civil liberties and establishes appropriate roles for government agencies and departments. CISA reflects sound compromises among many parties on these issues.[2]

CISA called for the Department of Homeland Security (DHS) to establish a "capability and process" (aka a portal) in the department to receive CTIs and DMs shared by businesses with the federal government in an electronic format—i.e., through email or media, an interactive form on an Internet website, or a real-time, automated process. In March 2016, DHS launched an Automated Indicator Sharing (AIS) platform that enables the government and the private sector to exchange cybersecurity threat information with one another.[3] The AIS initiative reportedly has more than 100 participants—spanning the banking, energy, and technology sectors, as well as both small and large companies—up from 6 participants this past spring.

Groups have begun testing their ability to share and receive indicators, but there is not yet sharing on a massive scale. The platform uses technical specifications, including the Trusted Automated eXchange of Indicator Information (TAXII), which defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information. It also uses Structured Threat Information eXpression (STIX), a collaborative effort to develop a structured language to represent threat information.[4]

An industry participant at last week's (June 9) CISA implementation workshop captured the thinking of many when he said, "Our adversaries are employing automated techniques against us. Machine-to-machine sharing is a key element needed to help solve our cybersecurity problems." He added that the United States cannot succeed if we pit cyber professionals—which are a significantly limited workforce asset—against machines.

CHAMBER PROMOTING CISA AS PART OF OUR NATIONAL CYBER CAMPAIGN

The Chamber is championing CISA as part of our national cybersecurity campaign. The Chamber will develop a document in concert with industry groups and other parties, including DHS and the Department of Justice (DOJ), that summarizes the CISA/AIS program, describes participants' protections and obligations, and urges the private sector to get involved in the AIS network. Appropriate, real-time automated sharing will strengthen the security and resilience of industry and government, thus heightening the costs of executing malicious attacks by U.S. adversaries. Many experts contend that the timely sharing of cyber indicators among various information-sharing and analysis organizations (ISAOs), information-sharing and analysis centers (ISACs), and private- and public-sector entities can reduce both the probability and the severity of cybersecurity incidents. (ISACs are considered to be ISAOs.)

The Chamber launched our cybersecurity roundtable series in 2014. This national initiative recommends that businesses of all sizes and sectors adopt fundamental Internet security

practices, including using the framework and similar risk management tools, engaging cybersecurity providers, and partnering with law enforcement before cyber incidents occur. Nine regional roundtables and two summits in Washington, D.C., have been held since 2014. More events are planned this year, including in San Antonio, Texas, on June 28 and in Chicago (Schaumburg, Illinois) on July 12. The Chamber's *Fifth Annual Cybersecurity Summit* will be held on September 27.

Each regional event includes approximately 200 attendees and typically features cybersecurity principals from the White House, DHS, the National Institute of Standards and Technology (NIST), and local FBI and Secret Service officials.

CISA IMPLEMENTATION GUIDANCE AND PROCEDUERS: A GOOD START

The enactment of CISA triggered an array of government guidelines and procedures. The Chamber has tracked implementation dates and monitored agencies' progress toward meeting the deadlines—and DHS and the DOJ delivered.

In particular, DHS and DOJ released interim guidance in February 2016 to assist "non-federal entities"—including organizations in the private sector and state and local governments—to share CTIs with the federal government. The departments also released interim procedures relating to the receipt and use of CTIs by the federal government, interim guidelines relating to privacy and civil liberties in connection with the exchange of these indicators, and guidance to federal agencies on sharing information in the government's possession.

At the time of this writing, the Chamber expects that DHS and DOJ officials will release by June 15 final procedures and guidance, which we generally agree with. We anticipate that the departments will accommodate the Chamber's request to clarifying the protections afforded to a non-federal entity when it shares cyber threat information with another non-federal entity. The Chamber and public authorities have a mutual interest in ensuring that the important protections authorized under CISA are clearly stated and utilized.

LOOKING AHEAD: PROMOTING CISA, BUILDING AND MAINTAING TRUST

Looking forward to the next several months, the Chamber believes that businesses' use of the CISA program arguably falls into roughly four categories. I want to emphasize that these groups are generalizations—shorthand for where private entities are in the information-sharing ecosystem.

- **Early Information-Sharing Leaders: Increasing the Quality and Volume of Sharing Under CISA.** Private organizations in this category are actively engaged in sharing threat data. They were in the vanguard of businesses establishing and funding ISAOs and ISACs several years ago. Companies in this grouping have long-established information-sharing relationships among multiple industry peers and government partners, and several of them are already directly connected to sharing programs like AIS.[5]

  CISA should give the lawyers and risk management professionals in these top organizations added certainty to receive CTIs and DMs and to share them with business

and the government. A core purpose of the new law is to extend liability protections to companies to encourage them to share cyber threat information.[6]

Companies in this category are eager to see a sea change in the real-time sharing of threat indicators within and across sectors, as well as between government and businesses. According to a Chamber member who addressed on May 16 the Commission on Enhancing National Cybersecurity, "Our adversaries should only use an attack or technique once. If our business spots an attack today, all businesses should be protected against it by day's end." Clearly, this company is an active member of the sharing community and wants public-private capacity to expand their capability to exchange threat data immediately. The Chamber agrees.

- **ISAOs/ISACs Members: Leveraging the Expanding Network of Sharing Conduits.** Many members in this dispersed network of ISAOs/ISACs do not share cybersecurity threat data directly with the government. Instead, rank-and-file members in this category typically share CTIs and DMs with other businesses and with the government through the channels that information bodies (e.g., the Financial Services-ISAC, the Oil and Natural Gas–ISAC) provide. This category is expected to swell as confidence in the CISA program grows and new information-sharing organizations are stood up over the coming months and years.

  The comparatively new ISAO standards organization is a key component of the Obama administration's cybersecurity strategy, launched in early 2015.[7] The administration's promotion of ISAOs is designed to encourage the protected sharing of information based on emerging and evolving threats that transcend industry sectors and geographic regions.[8] CISA is expected to have a positive influence on the expansion of the community of ISAOs and ISACs.

- **The Intrigued But Cautious: Sharing Should Pick Up as Both Education and Confidence Increase.** Businesses in this category have probably heard something about CISA through social media, cybersecurity events, and colleagues. Business leaders are interested in protected sharing arrangements, yet they are not ready to commit to routine sharing and receiving. Perhaps they do not know how to begin. The former view is due to misgivings about CISA's protections. The latter situation can be addressed through outreach and education.

  Many cautious businesses have pictures in their heads of bureaucrats lying in wait with regulations and privacy groups readying law suits. The Chamber does not agree completely with these perspectives, but we hear them expressed frequently. I attended a DHS-led C3 Voluntary Program in early June in Indianapolis and one individual's remark comes to mind. He said, "I have heard about CISA. But we are not ready as a company to participate—it will take a cultural shift." This person's apprehension tells us how central it is that trust in CISA's protections be earned and maintained. The Chamber and most government leaders appreciate that business attitudes change over time and participation in CISA/AIS will be gradual.

One change that may accelerate the use of CISA is business contracting arrangements. The Chamber foresees situations where large firms require their supply chain partners to belong to an ISAO/ISAC and to utilize AIS or some other automated means of timely indicator sharing.

- **Small Businesses and Underresourced Organizations: Indirect Beneficiaries of Innovations in Sharing.** Many small and midsize businesses, especially underresourced enterprises, will be able to benefit from an innovative, automated sharing ecosystem. A key long-term goal of information-sharing legislation is to foster economies of scale in real-time sharing. The Chamber anticipates that the marketplace will eventually provide inexpensive and easy-to-deploy technologies that conform to CISA's rules (e.g., scrubbing privacy information from CTIs) and generate and swap threat signatures at Internet speeds. Systems like AIS will be able to block attacks sooner and more regularly, compared with the relatively human-intensive sharing schemes in use today.

CISA FITS WITHIN A COLLECTION OF POLICY ISSUES THAT NEED ATTENTION

The Chamber is a strong supporter of CISA and its potential to clear away real or perceived hurdles to information sharing. CISA is not a silver-bullet solution to our nation's cybersecurity challenges. However, Chamber members say that increasing the speed and quality of bilateral information flows of CTIs and DMs is essential for developing a holistic approach to cyber defense. CISA is part of a mix of cybersecurity policies that need to advance together.

Here are some select issues that are worth highlighting for the full committee:

First, the joint industry-NIST *Framework for Improving Critical Infrastructure Cybersecurity* (the framework) is a sound baseline for businesses' cybersecurity practices. The CISA program and the framework are highly complementary. Businesses implement a cybersecurity risk management program before investing in information-sharing programs. In February 2016, the Chamber sent a letter to NIST, commenting on the framework.

Key points that the Chamber made in the letter include the following:

- The Chamber has been actively promoting the framework.
- Chamber members are using the framework and urging business partners to manage cybersecurity risks to their information networks and systems.
- The Chamber urges policymakers to help agencies and departments with streamlining existing regulations with the framework and maintaining the framework's voluntary nature.
- Industry opposes the creation of new or quasi-cybersecurity regulations, particularly when government authorities have not taken affected entities' perspectives into account.[9]

The bottom line: The Chamber values the Obama administration's leadership on the nonregulatory framework and urges the next administration to actively support it. NIST did an admirable job working with industry to development the tool. As framework stakeholders begin the yearlong transition from the Obama administration to its successor, the Chamber wants to

sustain the view held by most businesses and policymakers that the framework is a policy and political cornerstone for managing enterprise cybersecurity risks and threats.

To sustain the momentum behind the framework, the Chamber believes that both industry and government have jobs to do. On the one hand, the Chamber has been actively promoting the framework since it was released in 2014. Our national cybersecurity campaign is funded through members' sponsorships and through the contributions of state and local chambers of commerce, other business organizations, and academic institutions. Further, Chamber members are using the framework and urging business partners to manage cybersecurity risks to their data and devices. Industry is working with government entities, including DHS, to strengthen their information networks and systems against malicious actors.

On the other hand, the Chamber urges policymakers to help agencies and departments with harmonizing existing regulations with the framework and maintaining the framework's voluntary nature. Our organization opposes the creation of new or quasi-cybersecurity regulations, especially when government authorities have not taken affected entities' perspectives into account.

Second, the Chamber is engaging policy issues that ultimately relate to cybersecurity information sharing.

- The Chamber supports piloting a **CIDAR, shorthand for a cyber incident data and analysis repository**. In May 2016, we sent a letter to DHS saying that (1) data submitted to a CIDAR need to be made anonymous, (2) additional sharing protections may be needed, and (3) an experimental CIDAR could offer tangible upsides to public- and private-sector cybersecurity. Comprehensive information about cyber events could assist insurers in expanding cyber coverage and in identifying cybersecurity best practices for their customers.

- The Chamber appreciates the efforts of the Congressional Cybersecurity Caucus, particularly Co-chairs McCaul and Langevin, to press the administration to renegotiate the **Wassenaar Agreement (WA) control language governing so-called intrusion software and surveillance items** aspects of a controversial international agreement to prevent the export of sophisticated hacking tools to repressive governments and criminal organizations.

  Industry and democratic governments have a mutual interest in keeping malicious software out of the hands of bad actors. But the 2013 WA control language governing so-called intrusion software and surveillance items takes a seriously wrong approach to cybersecurity.[10]

  WA officials are gathering from June 20 to 24 in Vienna, Austria, at the working-group level. Industry is urging officials to completely eliminate the controls on technology, software, and hardware. If deleting the controls is not possible, the Chamber and many others recommend that WA officials substantially narrow the scope of the control language and dramatically simplify the language in order to bring clarity and enable

compliance.[11] If the WA control language is not eliminated or at least adequately amended, it could have a powerfully (unintended) negative effect on the CISA program. Creating cybersecurity policies and laws in the WA environment lacks sufficient transparency and does not advance public-private partnerships at home and abroad.

- On June 8, the Chamber's board of directors approved a **policy statement on cybersecurity norms and deterrence**. The paper argues that despite the existence of written blueprints, such as ones related to global prosperity and defense, the U.S. cybersecurity strategy is seemingly uncertain—both to many in the private sector and our adversaries alike. The Chamber believes that policymakers need to refocus national and global efforts to heighten the costs on sophisticated attackers that would willfully hack America's private sector for illicit purposes.

  Public-private policymaking needs to spotlight increasing adherence to international norms and deterrence to reduce the benefits of conducting harmful cyber activity against the U.S. business community and the nation. The statement makes several policy endorsements. For instance, the Chamber contends that the United States and its allies should enhance businesses' situational awareness through protected information sharing.

RECOMMENDATIONS ON CONGRESSIONAL OVERSIGHT

The Chamber believes that the CISA program is off to a good start. The CISA/AIS implementation guidance documents will likely be finalized today. We look forward to reviewing them with our members. The Chamber appreciates the open and constructive discussions that we have had with DHS and DOJ officials. While oversight by Congress is crucial, it is too soon to make changes to the legislation. CISA does not need to be reauthorized for several years (i.e., September 2025).

The Chamber's public message is twofold:

- To policymakers we say thank you for getting the cybersecurity information-sharing legislation across the finish line. And we urge lawmakers and the administration to be industry's ally as they use the program. Companies need to feel that policymakers have their backs. It is important that businesses see that the protections granted by the law—including matters tied to limited liability, regulation, antitrust, and public disclosure—become real.

- To businesses we say that you should use the framework, join an ISAO/ISAC, and take advantage of the CISA/AIS system as appropriate. The Chamber urges the senior leaders of industry groups to promote these initiatives among their peers and constituencies.

The Chamber and many stakeholders worked diligently over several years to craft policy that would serve multiple interests—namely individuals' security and privacy. We believe that CISA will enable private organizations of all sizes and sectors to be more secure and resilient against America's cyber adversaries.

NOTES

[1] The cyber legislation was included in the Consolidated Appropriations Act, 2016 (P.L. 114-113). www.congress.gov/bill/114th-congress/house-bill/2029

[2] See Automated Indicator Sharing (AIS) resources, including the Cybersecurity Information Sharing Act of 2015 (CISA) implementation procedures and guidance, available at www.us-cert.gov/ais. Also see pro-CISA advocacy papers: "It's About Protecting America's Cyber Networks, Not Surveilling You" (August 10, 2015); "Sharing Cyber Threat Indicators (CTIs)—Separating Fact From Fiction" (August 19, 2015); "'Voluntary' Means Voluntary—Separating Fact From Fiction" (August 26, 2015); and "Going on the 'Defensive'—Separating Fact From Fiction" (October 5, 2015). http://insidecybersecurity.com/daily-news/info-sharing-debate-shifts-implementation-privacy-advocates-now-back-cyber-law

[3] www.us-cert.gov/ais

[4] http://blogs.wsj.com/cio/2016/03/21/homeland-security-department-launches-cyber-threat-sharing-platform

[5] www.dhs.gov/topic/cybersecurity-information-sharing

[6] http://insidecybersecurity.com/daily-news/mccaul-evaluate-effectiveness-cyber-info-sharing-law-including-liability-protections

[7] In February 2015, President Obama signed an executive order (EO) to promote cybersecurity information sharing among multiple business and government entities. The EO urges the private sector to develop information sharing and analysis organizations (ISAOs) to serve as focal points for cybersecurity information sharing and collaboration within the private sector and between the private sector and government. www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

[8] http://insidecybersecurity.com/daily-news/isao-standards-body-issue-next-round-draft-plans-info-sharing-july

[9] http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/20160209_US_Chamber_of_Commerce.pdf

[10] https://www.uschamber.com/sites/default/files/documents/files/final_group_letter_bis_proposed_rule_intrusion_software-surveillance_items_july_20_2015.pdf

[11] http://insidecybersecurity.com/daily-news/obama-administration-agrees-renegotiate-cyber-export-controls