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

***

Answers to Questions for the Record
November 4, 2016

Questions from Chairman John L. Ratcliffe

1. *Does the U.S. Chamber of Commerce believe that the Cybersecurity Act of 2015, specifically Automated Indicator Sharing, is applicable to all businesses, including small businesses, and private organizations?*

The Chamber believes that the Cybersecurity Act of 2015—particularly title I, the Cybersecurity Information Sharing Act of 2015 (CISA)—and Automated Indicator Sharing (AIS) are applicable to businesses and private organizations of all sizes and sectors.

2. *What avenues do government and industry have to increase businesses' awareness of the Cybersecurity Act of 2015, specifically Automated Indicator Sharing?*

    a. *Do you expect that all businesses, especially small ones, will use the Cybersecurity Act of 2015, specifically the Automated Indicator Sharing program, directly?*

There are many ways to publicly promote CISA. The Chamber led the Protecting America's Cyber Networks Coalition, a partnership of more than 50 leading business associations representing nearly every sector of the U.S. economy to pass CISA. Each association has on average thousands of members.

The Chamber is championing CISA as part of our cybersecurity campaign, which was launched in 2014. This national initiative recommends that businesses of all sizes and sectors adopt fundamental Internet security practices, including the joint industry-National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (the framework) and the new information-sharing law.

The Chamber spearheaded 11 major regional roundtables and 2 summits in Washington, D.C. More events are planned for 2017. The Chamber's Fifth Annual Cybersecurity Summit was held on September 27. Each regional event had approximately 200 attendees and typically features cybersecurity principals from the White House, Department of Homeland Security (DHS), NIST, and local FBI and Secret Service officials.

The Chamber also partners with state and local chambers and universities to produce cyber educational events in locations such as Appleton, Wisconsin; Augusta, Georgia; Oak Brook, Illinois; Indianapolis, Indiana; Irving, Texas; and Longview, Texas. We endorse CISA and AIS at each gathering. In addition, Chamber professionals regularly speak on and/or moderate industry panels tied to cybersecurity, where we can actively pitch CISA/AIS to multiple businesses.

DHS Deputy Secretary Ali Mayorkas addressed the Chamber's Small Business Summit on June 14, and he advocated that businesses take basic, prudent steps to protect their devices and sensitive data, including leveraging cybersecurity information-sharing services.

Big picture: The Chamber is urging businesses to use the framework, join an information-sharing body, and take advantage of the CISA/AIS system as appropriate. We are pressing senior leaders of industry groups to popularize these initiatives among their peers and constituencies, including through jointly written Chamber-DHS op-ed articles.[1]

The Chamber commends DHS and the Department of Justice (DOJ) for jointly holding their Cybersecurity Conference for Lawyers on September 28, which included a discussion on traditional challenges to sharing threat data and CISA's attempt to address these challenges and a demonstration of the AIS program.

3. *The issue of how many entities are signed up for the Automated Indicator Sharing program was discussed at the hearing. Should Information Sharing and Analysis Organizations (ISAO)- and Information Sharing and Analysis Centers (ISAC)-participating entities be included in the accounting of the number of participating entities under the program if they are sharing cyber threat data through an ISAO or ISAC that is plugged into DHS' NCCIC?*

First, it is important to stress the Chamber believes that the success of CISA and AIS should *not* be linked to the number of organizations that sign up for AIS. Some subcommittee members suggested at the hearing that the number of AIS signers and the achievements of CISA/AIS are bound together. Most industry organizations are unlikely to share cyber threat indicators (CTIs) directly with government partners. Instead, the Chamber believes that the vast majority of businesses will share and receive cyber threat data with industry peers and ISACs and ISAOs. It is our understanding that most businesses will use information-sharing bodies as conduits between themselves and DHS, among other federal entities. These businesses will not be signed up with AIS, but significant amounts of information sharing will nonetheless take place.

Second, ISAOs and ISACs and their respective members should be part of the calculation of private organizations that are possibly using CISA/AIS. The Chamber defers to DHS' data concerning AIS involvement. Yet at the time of this writing, we understand that approximately 150 private organizations have signed DHS' Terms of Use that govern the use of CTIs and DMs and participation in the AIS initiative.[2] Fifty-eight (58) of these organizations are attached to the AIS server and consume government-furnished CTIs. In addition, 12 of these organizations are either ISACs or ISAOs. For instance, the Financial Services-ISAC (FS-ISAC) has upward of 7,000 member financial institutions and partner organizations. Presumably, many of these entities are engaged in protected information sharing under CISA but may not be part of AIS accounting.[3]

Similarly, the Health Information Trust Alliance (HITRUST) Cyber Threat XChange, the health industry's ISAO, is now connected to AIS and supports the bidirectional sharing of cyber threat data with DHS. The real-time sharing of CTIs between HITRUST's more than 1,000 members and DHS helps private-sector organizations reduce their cyber risks.[4]

The Chamber understands that several entities are testing the sharing process before they initiate automated, bidirectional sharing on routine basis.

Questions from Ranking Member Cedric L. Richmond

4. *In accordance with §103 and §105(a)(4) of the Cybersecurity Act of 2015 (P.L. 114-113), on June 15, 2016, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General issued updated, final guidance on the sharing of cyber threat indicators and defensive measures among multiple federal and nonfederal entities.*

   a. *What was your impression of the guidance? Are there aspects that you find insufficient or impractical?*

The Chamber was impressed at the widespread support CISA/AIS stakeholders showed for the final CISA procedures and guidance documents that were released on June 15. The Chamber especially commends DOJ's Leonard Bailey, senior counsel, and DHS' Gabe Taran, acting assistant general counsel for infrastructure programs, for their positive roles in negotiating with multiple parties and writing the documents under a tight deadline.

The Chamber believes that the procedures and guidance are sufficient and practical.

   b. *In addition to resolving the question of liability protections for private-to-private sharing, are there other aspects of the DHS guidance that you believe would benefit from additional clarity?*

The issue related to clarifying liability protections for private-to-private sharing seems to have been dealt with adequately. The procedures and guidance do not need additional clarification at this time. In the main, the Chamber is urging industry to take advantage of CISA/AIS as appropriate.

   c. *Are there aspects of the law that should be clarified?*

No. The CISA/AIS program is off to a good start. While oversight by Congress is crucial, it is too soon to make changes to the legislation. CISA does not need to be reauthorized until September 2025.

The Chamber urges lawmakers and the next administration to be industry's ally as it uses CISA/AIS, which is currently more important to businesses than clarifications. Companies need to trust that policymakers have their backs. It is important that businesses see that the protections granted by CISA—including matters tied to limited liability, regulation, antitrust, and public disclosure—become real. For some businesses, the protections are still an open question.

The Chamber agrees with a witness who spoke on June 21 before the Commission on Enhancing National Cybersecurity at the University of California-Berkeley. He noted that the government could make it easier for companies to create a "regulatory safe space," where they can more effectively share information about threats and attacks.[5]

The Chamber hears such sentiments frequently and believes that government entities like DHS want to use company data prudently. However, many more agencies and departments will have to adopt attitudes and actions that do not discourage businesses from reporting threat and vulnerability data.

5. *As a general rule, small and medium-size businesses do not have the resources to devote to the most advanced, state-of-the-art information technology systems. As such, smaller enterprises may use older systems that have known cybersecurity vulnerabilities. Can these companies rely on older systems to share or receive threat information or do their platforms require a more advanced system?*

The Chamber's experience suggests that sophisticated cybersecurity programs can be very expensive to develop, deploy, and maintain for companies of all sizes, particularly small and midsize businesses (SMBs).

DHS does not charge a fee for companies to participate in AIS. However, any AIS participant will need to adhere to defined technical connectivity activities, which DHS helps organizations manage.[6] Larger firms may have more resources to submit indicators directly through AIS. Most SMBs may not need to.

Indeed, the Chamber anticipates that many SMBs will benefit from an innovative, automated-sharing ecosystem. A key long-term goal of information-sharing policy is to foster economies of scale in real-time, machine-to-machine 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.

The Chamber understands that cyber threat intelligence companies have the means to enable companies to opt-in to AIS and gain from the process of receiving pertinent security event information such as IP addresses, domain names, hashes, and actor tactics, techniques, and procedures.

From a resource standpoint, it is probably too much to ask most SMBs to engage in the cybersecurity threat-sharing ecosystem directly. Many SMBs will likely struggle to create and maintain sound cybersecurity programs.[7] Technology may be challenging to use, and professional cyber talent is both scarce and pricey. Public policy does not do a sufficient job of recognizing the potentially extraordinary costs that industry faces in creating robust information-security programs.

Secretary of Commerce Penny Pritzker spoke at the Chamber on September 27 concerning cybersecurity policy. She said that cyberspace is the "only domain where we ask private companies to defend themselves" against foreign powers and other significant threats. She wondered aloud, "Does that sound as crazy to you as it does to me?"[8] Government does not stand between private entities and malicious hackers, she suggested.

It is instructive, according to a Council of Insurance Agents and Brokers market survey, that 26.1% of SMBs purchase "cyber" insurance for risk mitigation assistance (4.5%) and post-breach resources (21.6%). In contrast, 20.4% of large entities purchase "cyber" insurance for risk mitigation assistance (10.2%) and post-breach resources (10.2%).[9] In the Chamber's view, companies typically have healthy and maturing cyber risk management programs in place before engaging in active information-sharing initiatives.

6. *In developing the aforementioned guidance, §103(a)(5) specified that the procedures established must facilitate periodic circulation of cybersecurity "best practices" designed with special attention to the accessibility and implementation challenges faced by small businesses. Do the policies and procedures described in the guidance actually facilitate the development and circulation of best practices that are mindful of small business needs?*

In keeping with section 103(a)(5) of CISA, the federal government-sharing guidance calls for the periodic sharing of cybersecurity best practices "with attention to accessibility and implementation challenges faced by small business concerns." The guidance outlines several programs, activities, and federal agencies and departments that support the recurrent sharing of sound cybersecurity techniques, which are expected to be rooted in the ongoing analyses of cyber threat data.

Here are some examples of cybersecurity best practices featured in the federal government-sharing guidance and that the Chamber includes in our national cyber education campaign:

- **NIST Computer Security Division.** NIST special publications and interagency reports, covering a broad range of topics, provide management, operations, and technical security guidelines for federal agency information systems. Beyond these documents, which are peer reviewed throughout industry, government, and academia, NIST conducts workshops, awareness briefings, and outreach to help ensure greater understanding of standards and guidelines resources.[10]

- **DHS Critical Infrastructure Cyber Community (C^3) Voluntary Program.** The C^3 (pronounced "c cubed") Voluntary Program helps enhance critical infrastructure cybersecurity and encourage the adoption of the framework. The C^3 Voluntary Program aids sectors and private organizations that want to use the framework by connecting them with cyber risk management tools offered by DHS, other federal entities, and the private sector.[11]

- **DHS National Cybersecurity and Communications Integration Center (NCCIC).** The NCCIC disseminates publications that recommend practices and standards for technical and nontechnical users. Information is available for government users, as well as owners, operators, and vendors of industrial control systems.[12] In addition, the NCCIC includes information specifically focused on securing small business and home networks.[13]

  Through the US-CERT, a component of NCCIC, DHS offers the Cyber Resilience Review (CRR), a no-cost, voluntary, nontechnical assessment to help an organization evaluate its resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals.

- **Small Business Administration (SBA) cybersecurity website.** The SBA provides information about cybersecurity best practices through its website, which features top tips, among other resources, that SMBs can use.[14]

7. *There is a natural tension between sharing threat indicators quickly to facilitate rapid response, and sharing only the most valuable information once it has been processed and analyzed. I understand that DHS uses the former, emphasizing volume and timeliness. Do you prefer this "time is of the essence" approach? In other words, how useful and actionable is the information you [a business or private organization] receive from DHS?*

The Chamber supports the "time is of the essence" mind-set. During the legislative debate concerning CISA, we opposed amendments that would attempt to address the "second scrub" issue by requiring DHS to perform another scrub of cyber threat data for personal information before disseminating indicators to appropriate federal entities. So the speed of sharing is key.

Granting authority to DHS to conduct a second scrub is not inherently bad if viewed only through the vague lens of "privacy." But privacy is just one of several considerations in CISA. For example, when one understands that CTIs rarely if ever contain personal information, the second scrub would bog down the sharing of CTIs from businesses to the federal entities that need them in a timely manner.[15]

A DHS privacy official said at the Cybersecurity Conference for Lawyers in September that if a CTI field "fails or is not completed fully" by a submitter, the whole indicator is not held back, which is constructive from a timeliness standpoint.[16]

8. *The Cybersecurity Act of 2015 contains numerous provisions designed to safeguard privacy and civil liberties by requiring, for instance, the scrubbing of personal information. Are private sector organizations using their own systems to fulfill these obligations or relying on DHS mechanisms?*

Section 104(d)(2) of CISA requires businesses to remove any information from a CTI or DM that it knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual who is not directly related to a cybersecurity threat before sharing that data with a federal entity.[17]

Private organizations use their own technical capabilities to scrub indicators of personal information. It is worth noting that a DHS privacy official said at the Cybersecurity Conference for Lawyers that there is no "hard and fast list of privacy information that must be removed" from CTIs. CISA/AIS stakeholders need to consult the nonfederal entity guidance for scrubbing protocols. Scrubbing is "ultimately up to the company that is sharing the indicators," she added. The Chamber instructs businesses to remove personal information from cyber threat data and not to rely on DHS mechanisms, which, among other things, may impede timely sharing efforts.

Notes

[1] http://thehill.com/blogs/congress-blog/technology/304163-cybersecurity-building-resiliency-together, www.csoonline.com/article/3124626/security/advancing-cybersecurity-through-automated-indicator-sharing.html

[2] www.us-cert.gov/sites/default/files/ais_files/AIS_Terms_of_Use.pdf

[3] http://media.wix.com/ugd/416668_2c6d85d4964743f8b4d3470b860f6e3b.pdf

[4] https://hitrustalliance.net/hitrust-advances-state-cyber-threat-information-sharing-nations-healthcare-sector

[5] https://cltc.berkeley.edu/2016/06/27/cltc-hosted-white-house-commission-considers-challenges-opportunities-for-the-next-president.

[6] www.us-cert.gov/sites/default/files/ais_files/AIS_fact_sheet.pdf, www.us-cert.gov/sites/default/files/ais_files/AIS_FAQ.pdf

[7] https://inthenation.nationwide.com/news/small-business-cyber-security-survey

[8] www.commerce.gov/news/secretary-speeches/2016/09/us-secretary-commerce-penny-pritzker-delivers-keynote-address-us

[9] www.ciab.com/news.aspx?id=6176

[10] www.nist.gov/itl/computer-security-division

[11] www.dhs.gov/ccubedvp

[12] https://ics-cert.us-cert.gov

[13] www.us-cert.gov/home-and-business

[14] www.sba.gov/cybersecurity

[15] www.uschamber.com/sites/default/files/cisa_ctis_separating_fact_from_fiction_aug_19_final.pdf

[16] www.us-cert.gov/sites/default/files/ais_files/AIS_Submission_Guidance_Appendix_A.pdf

[17] www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf