U.S. CHAMBER OF COMMERCE

Ann M. Beauchesne
Senior Vice President
National Security and Emergency Preparedness

1615 H Street, NW
Washington, DC 20062
202-463-3100

January 12, 2018

Dr. Greg White
Executive Director, ISAO Standards Organization
Executive Director, Center for Infrastructure Assurance and Security
The University of Texas at San Antonio
Greg.White@utsa.edu

Allen Shreffler
Deputy Director, ISAO Standards Organization
Senior Cybersecurity Analyst, LMI
ashreffler@lmi.org

Rick Lipsey
Advisor, ISAO Standards Organization
Senior Strategic Cyber Lead, LMI
rlipsey@lmi.org

Subject: Solicitation for a Discussion on an ISAO Certification Model

Dear Dr. White, Mr. Schreffler, and Mr. Lipsey:

The U.S. Chamber of Commerce appreciates the opportunity to respond to the Information Sharing and Analysis Organization Standards Organization's (ISAO SO's) December 1, 2017, *Solicitation for a Discussion on an ISAO Certification Model*.[1]

The Chamber and the ISAO SO have a strong, mutual interest in furthering the awareness of, and participation in, cybersecurity information sharing efforts. This past October, the Chamber was pleased to host ISAO SO leadership at its *Sixth Annual Cybersecurity Summit* and speak at the ISAO SO's inaugural *International Information Sharing Conference*. Our two organizations share the widely held view that U.S. economic and national security are strengthened as businesses build and improve their cyber risk management programs. Indeed, leading cyber stakeholders believe that information sharing should be a central part of businesses' overall cybersecurity practices.

However, while advocating for cyber information sharing policy over the past several years, the Chamber has experienced no groundswell among its members and information sharing bodies in support of certifying ISAOs and information sharing and analysis centers (ISACs).

SUMMARY: THE CHAMBER AND THE ISAO SO SHARE THE GOAL OF ADVANCING CYBER INFORMATION SHARING, BUT CERTIFICATIONS WILL NOT STRENGTHEN TIMELY, QUALITY SHARING

- The Chamber and the ISAO SO share a robust interest in furthering businesses' active involvement in cybersecurity information sharing activities.
- Industry has not expressed a demand for certifying information sharing and analysis organizations (ISAOs) and information sharing and analysis centers (ISACs).
- Businesses stress to the Chamber that certifications would harm the top goals of practitioners, which include maintaining flexibility and advancing timely and context-rich data sharing efforts.

First, the Chamber helped lead the development and passage of legislation like the Cybersecurity Information Sharing Act (CISA) from approximately 2011 to 2015. During this period, no industry group told the Chamber that ISAO certifications would markedly help business or government information sharing objectives.[2] Large swaths of industry did not expend considerable time and resources to achieve this legislative breakthrough, which the ISAO SO is leveraging, only to see quasi-regulatory certification schemes come to fruition.

Second, the ISAO SO's push for certification models contrasts sharply with industry's original understanding that ISAOs would not need to be certified against baseline information sharing standards. In January 2015, the Chamber hosted White House National Security Council (NSC) officials to discuss a forthcoming executive order (EO) on information sharing, which urged the sharing of cyber threat data within the private sector and between the private sector and government. NSC authorities noted that early drafts of the EO contemplated a certification model for ISAOs, but the requirement was abandoned because it was unhelpful and controversial. In addition, the pending EO seemed to downplay the important roles that ISACs, which are anchored to critical infrastructure sectors, have historically played in favor of ISAOs.[3]

To be sure, Chamber members expressed a healthy mix of support for and skepticism about the EO. On the one hand, the EO specifically called for leveraging ISAOs to serve as "hubs" through which communities of interest could receive and distribute information. "As more communities develop their own hubs," White House authorities suggested that they could "communicate efficiently between hubs and create a prosperous cycle of information sharing," which is a constructive viewpoint.[4] The Chamber generally supported the thinking behind the EO, which made particular sense in 2015—a year in which both public and private actors made a big push to pass CISA.

On the other hand, back in 2015 and continuing through today, Chamber members consistently voiced intense misgivings that the creation of an ISAO SO[5] would lead to the furtherance of certification schemes—putting ISAOs, according to one individual, in a "conceptual box, wrapped in red tape." Many ISAO stakeholders stressed to the Chamber that

certifications would do little to advance timely and context-rich data sharing—which are the most frequently articulated goals of cyber practitioners.[6]

Third, in September 2016, the ISAO SO released an initial set of voluntary guidelines. The group intentionally did not include language on "minimum requirements" or the role of "certification" for ISAOs, which was a positive development.[7] The Chamber communicated to both DHS and ISAO SO principals that it is too early in the process to certify and set minimum requirements for information sharing bodies.[8] Many in industry argued that mandates would restrict, not enhance, the progress of ISAOs.[9] Business principals tell the Chamber that certification models constitute a "solution that's in search of a problem."

Fourth, the Chamber had a constructive discussion with ISAO SO leaders in December. They earnestly emphasized that certifications would be crucial to increase trust among multiple ISAO participants. Indeed, the December 1 solicitation suggests, "As the number of ISAOs grows from dozens to hundreds, a clear understanding of an ISAO's services and capabilities will be essential to promote the *growth of trust* that is essential to facilitate the rapid propagation of time-critical information throughout the ecosystem" [italics added].

Trust is an important ingredient found among the people and institutions that comprise an information sharing body. Nevertheless, the Chamber strongly believes that certification arrangements, which suggest costly and regulatory qualities, are neither a prudent nor a workable means to achieve the goal of increasing confidence in an ISAO. Certification regimes are unlikely to foster the progress of ISAOs and, instead, are more apt to be a distraction to many. What's more, it is realistic to think that over time, certifications would conflict with CISA procedures and guidance and the evolution of the DHS-administered Automated Indicator Sharing, or AIS, program, which would be a significantly troublesome outcome.[10]

The Chamber values the ISAO SO's work to catalyze information sharing networks. However, it strongly opposes the certification of ISAOs and ISACs, which the Chamber urges the ISAO SO to respect.

***

The Chamber appreciates the opportunity to offer its views to the ISAO SO concerning its certification proposal. If you have any questions or need more information, please do not hesitate to contact me (abeauchesne@uschamber.com, 202-463-3100) or my colleague Matthew J. Eggers (meggers@uschamber.com, 202-463-5619).

Sincerely,

Ann M. Beauchesne
Senior Vice President

Matthew J. Eggers
Executive Director, Cybersecurity Policy

Endnotes

[1] www.isao.org/drafts/solicitation-for-a-discussion-on-an-isao-certification-model, https://www.isao.org/wp-content/uploads/2017/12/ISAO-SO-Solicitation-for-ISAO-Certification-Model.pdf

[2] DHS, "Frequently Asked Questions About Information Sharing and Analysis Organizations (ISAOs)," (October 6, 2016). https://www.dhs.gov/isao-faq

[3] Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing* (February 13, 2015). https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

[4] White House blog, *Promoting Private Sector Cybersecurity Information Sharing* (September 3, 2015). https://obamawhitehouse.archives.gov/blog/2015/09/03/promoting-private-sector-cybersecurity-information-sharing

[5] DHS blog, *DHS Awards Grant for Creation of the Information Sharing and Analysis Organization (ISAO) Standards Organization (SO)* (September 3, 2015). www.dhs.gov/blog/2015/09/03/dhs-awards-grant-creation-information-sharing-and-analysis-organization-isao

[6] DHS Office of Inspector General, *Biennial* Report *on* DHS' *Implementation of the Cybersecurity Act of 2015, OIG-18-10* (November 1, 2017). www.oig.dhs.gov/sites/default/files/assets/2017-11/OIG-18-10-Nov17_0.pdf

[7] www.isao.org/news-updates/isao-so-releases-initial-voluntary-guidelines

ISAO standards group sidesteps 'minimum requirements' in its upcoming guidance," *Inside Cybersecurity* (August 30, 2016). http://insidecybersecurity.com/daily-news/isao-standards-group-sidesteps-minimum-requirements-its-upcoming-guidance

[8] "Creating trust through certification for cyber info-sharing remains an open question," *Inside Cybersecurity* (September 6, 2016). http://insidecybersecurity.com/daily-news/creating-trust-through-certification-cyber-info-sharing-remains-open-question

In October 2016, the Chamber urged DHS to remove references to accrediting and certifying ISAOs from the draft *National Cyber Incident Response Plan*, or NCIPR, which the department apparently agreed to. www.uschamber.com/sites/default/files/documents/files/10-31-16_uscc_letter_re_draft_ncirp_final.pdf

DHS, which is funding the ISAO SO, is reportedly neutral on the issue of ISAO certifications. Instead of acting disinterestedly, the Chamber urges the department to discourage the certifications portion of the ISAO SO's work.

[9] "Industry groups say cyber info-sharing efforts could be hampered by 'certification' plan," Inside Cybersecurity (November 10, 2017). https://insidecybersecurity.com/daily-news/industry-groups-say-cyber-info-sharing-efforts-could-be-hampered-certification-plan

[10] CISA procedures and guidance via DHS' Automate Indicator Sharing, or AIS, program, www.us-cert.gov/ais

"How DHS' automated information sharing program continues to evolve, grow (December 29, 2017), *Federal News Radio*. https://federalnewsradio.com/dhs-15th-anniversary/2017/12/how-dhs-automated-information-sharing-program-continues-to-evolve-grow