TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 N. Courthouse Rd., Suite 200
Arlington, VA 22201 USA
www.tiaonline.org
Tel: +1.703.907.7700
Fax: +1.703.907.7727

Submitted via ISAO@hq.dhs.gov and www.regulations.gov

July 10, 2015

Mr. Michael Echols
Director, JPMO-ISAO Coordinator
NPPD, Department of Homeland Security
245 Murray Lane, Mail Stop 0615
Arlington VA 20598-0615.

Re: Docket No. DHS-2015-0017, *Notice of Request for Public Comment Regarding Information Sharing and Analysis Organizations*

Dear Mr. Echols:

The Telecommunications Industry Association ("TIA") hereby submits comments in response to the Department of Homeland Security's ("DHS") request for comment[1] on the formation of Information Sharing and Analysis Organizations[2] ("ISAOs") for cybersecurity information sharing, as directed by Executive Order 13691.[3] TIA appreciates the opportunity to provide input on the formation of ISAOs and the best practices that will guide them.

TIA represents hundreds of ICT manufacturer, vendor, and supplier companies in government affairs and standards development. Numerous TIA members are

---

1 *See Notice of Request for Public Comment Regarding Information Sharing and Analysis Organizations*, Request For Public Comment, 80 FR 30258 (May 27, 2015).

2 ISAOs are defined in Sec. 212(5) of the Homeland Security Act of 2002.

3 *See* Exec Order No. 13691, Promoting Private Sector Cybersecurity Information Sharing (February 13, 2015), *available at* https://www.federalregister.gov/articles/2015/02/20/2015-03714/promoting-private-sector-cybersecurity-information-sharing ("EO 13691").

companies producing ICT products and systems, creating information security-related technologies, and providing ICT services information systems, or components of information systems. These products and services are directly impacted by Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing*.[4] Representing our membership's commitments in this area, TIA holds membership and is actively engaged in key public-private efforts that contribute to secure information systems, including the Federal Communications Commission's ("FCC") Communications Security, Reliability, and Interoperability Council ("CSRIC"); the Communications Sector[5] and Information Technology Sector[6] Coordinating Councils; and the National Coordinating Center for Communications ("NCC"), the Information Sharing and Analysis Center ("ISAC") for telecommunications, part of the DHS National Cybersecurity and Communications Integration Center ("NCCIC").[7]

Through its Cybersecurity Working Group, TIA members engage in policy advocacy consistent with the following principles:

- Public-private partnerships should be utilized as effective vehicles for collaborating on current and emerging threats.
- Industry-driven best practices and global standards should be relied upon for the security of critical infrastructure and supply chains.
- Voluntary private sector security standards should be used as non-mandated means to secure the ICT supply chain.
- Governments and businesses should be allowed to provide more timely and detailed cyber intelligence amongst and between the public and private sectors to help identify threats to protect private networks.

---

[4] The National Institute of Technology and Standards (NIST), *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0* (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf ("NIST Cybersecurity Framework").

[5] http://www.commscc.org/

[6] http://www.it-scc.org/

[7] http://www.dhs.gov/national-coordinating-center-communications

- Cybersecurity funding for federal research efforts should be prioritized.

TIA appreciates DHS' efforts to enable and facilitate "private companies, nonprofit organizations, and executive departments and agencies…to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible,"[8] and looks forward to working with DHS and other governmental stakeholders moving forward. TIA offers the specific input below based on the consensus views of TIA's hundreds of ICT manufacturer, vendor, and supplier member companies, in response to each question posed to the extent possible.

I. TIA RESPONSES TO SPECIFIC QUESTIONS POSED IN THE DHS REQUEST FOR INFORMATION

A. Question 1: Describe the overarching goal and value proposition of Information Sharing and Analysis Organizations (ISAOs) for your organization.

TIA is supportive of Executive efforts to improve the sharing of timely cyber-based threat information amongst and between government and industry stakeholders. As the number and diversity of cyber threats to both the public and private sector continue to increase, it is more important than ever for the enablement of voluntary real-time bi-directional sharing in any way possible.

TIA believes that an overarching priority in the formulation of ISAOs should be to ensure that ISAOs are additive to efforts to improve information sharing, building on the success of existing public-private partnerships, particularly the ISAC model, to facilitate information sharing and to improve cooperation in defense against cyber attacks. As a long-standing member of the NCCIC/Comms-ISAC, TIA believes that an industry-driven approach would naturally ensure that there is no overlap in an ISAO's purpose or process in relation to an existing ISAC; while existing ISACs do meet the definition of an ISAO under the Homeland Security Act of 2012, the operation of ISACs should not be required to change due to the requirements on ISAOs. Ensuring flexibility in ISAO's approaches will allow ISAOs to address DHS-identified needs in the creation of ISAOs (*e.g.*, engagement with entities that cross critical

[8] EO 13691 at Sec. I.

infrastructure sectors, engagement with entities not currently part of one or more ISAC's process, needed differentiation in processes depending on an organization's requirements and abilities, prioritization of shared information, etc.).

Further, TIA notes that a key component that the ISAO concept cannot address at this time is the need for adequate liability protections for businesses sharing cybersecurity threat indicators, which also address privacy and civil liberty concerns.

Finally, TIA believes that the ISAO's role in information sharing should not be viewed as the end game. Rather, information sharing is a tool to achieve timely, reliable, and actionable situational awareness through information sharing and collaboration. DHS, along with other stakeholders, should continue to prioritize improvement in other important areas, such as enhanced cybersecurity research and development, workforce training and education, and public awareness.

B. Question 2: Identify and describe any information protection policies that should be implemented by ISAOs to ensure that they maintain the trust of participating organizations.

TIA believes that a cornerstone of success for ISAOs will be trust amongst participating organizations, which is facilitated by industry-led self-governance. ISAOs can provide trust to participating organizations by, among other means, working towards the following: vetting potential participating organizations for trustworthiness, giving clear and unambiguous liability protections to participating organizations to the maximum extent possible under the law, establishing transparent and predictable procedures for participation, and by consistently seeking and reasonably responding to feedback from participating organizations on how these processes can be improved.

C. Question 3: Describe any capabilities that should be demonstrated by ISAOs, including capabilities related to receiving, analyzing, storing, and sharing information.

Consistent with the above, the capabilities of an individual ISAO must differ depending on the needs of each ISAO's different constituents. For this reason, flexibility in the ISAO

framework (*e.g.*, the use of automated sharing may not be appropriate in all contexts) and standardized best practices is crucial. While each ISAO's capabilities will be different to reflect the needs of its membership, TIA agrees that the ISAO framework should contemplate the roles of providing clear guidelines for the submission of appropriate information in addition to aggregating that information, analyzing information received and organizing it into a standardized and actionable format with appropriate context, and disseminating such actionable information to qualified participating organizations through a hub-and-spoke model (*e.g.*, the NCCIC).

D. Question 4. Describe any potential attributes of ISAOs that will constrain their capability to best serve the information sharing requirements of member organizations.

To best serve the ISAO model's success, TIA believes that the government should ensure that it replicates the governance model found in ISACs. In ISACs, leadership, processes, etc. are governed by that ISAC's membership, and are in this way responsive to the needs of its sector's members. In addition, participation is voluntary, facilitating a collaborative approach that avoids any implied liability. This flexibility allows a system in which no two ISACs are identical, and TIA urges against an overly-prescriptive ISAO framework.

Furthermore, the danger of being disconnected from existing ISACs and other ISAOs, resulting in unnecessary duplication and waste of resources, can exist if the ISAO framework does not contemplate connectivity across the public-private partnership-based information sharing landscape. While DHS has provided some insight into the range of diversity it envisions across ISAOs, regardless of the context, if ISAOs develop into a siloed approach that creates duplication, this would disincentivize participation in ISAOs. In the context of ISACs, such issues may be addressed through the National Council of ISACs.

The ISAO framework and standards should also be informed by the perspective of small- and medium-sized entities ("SMEs"). A key goal for ISAOs should be to maximize participation by SMEs that typically do not have resources or staffing for full-time attention to cybersecurity

information sharing. TIA's membership, consisting of entities of all sizes, stands ready to work with DHS, the ISAO standards organization, and other stakeholders to help find this balance.

Lastly, TIA notes that the initiation of an ISAO is expected to be an expensive undertaking. It is important that the means by which an ISAO can initiate and sustain its activities from a resource perspective should be addressed. While DHS has publicly stated that it expects hundreds of ISAOs to form over the next two years, the source of resources to create this environment remains unclear. Without this aspect being addressed in the creation of an ISAO framework, TIA does not expect many ISAOs to take the initial steps towards their creation.

E. Question 5. Identify and comment on proven methods and models that can be emulated to assist in promoting formation of ISAOs and how the ISAO "standards" body called for by E.O. 13691 can leverage such methods and models in developing its guidance.

As noted above, we strongly urge for the methods of existing ISACs to be replicated in ISAOs. A key feature that the ISAO standards body should ensure it incorporates into its output should be the flexibility needed by ISAOs to best serve the needs of their membership. Initially, the ISAO standards body should carefully and deliberately examine each of the existing ISACs to create an inventory of the positive characteristics they find common to ISACs. For example, the Comms-ISAC is a robust and well-established information sharing process which has facilitated information sharing between industry and government, which ISAOs should leverage.

The framework for a successful ISAO should also reflect the success of the membership-driven approach to information sharing. More specifically, from the perspective of the ICT manufacturer, vendor, and supplier community, it is important that the United States government avoid being perceived as controlling an ISAO in order to encourage participation. Without process transparency, key aspects of trust will be lacking, and will decrease an ISAO's chance of success.

Furthermore, in the process by which the ISAO standards organization will develop best practices or ISAOs, TIA urges for a transparent, open, and accessible process. One way that DHS

can ensure these characteristics in the ISAO standards development process is to require the ISAO standard development organization's process to be accredited by the American National Standards Institute ("ANSI") or some equivalent construct. Voluntary consensus standards developed under processes such as ANSI's provide assurance that the standards represent the consensus agreement among stakeholders, provide fairness in process (notice, consideration of all concerns and contributions, etc.), and guarantee that any organization or individual has the opportunity to engage in the process and work with other stakeholders to shape the standard as needed. The ISAO standards should be technology-neutral based on best practices and methodologies from the existing ISACs, as well as industry-led international standards.

F. Question 6. How can the U.S. government best foster and encourage the organic development of ISAOs, and what should the U.S. government avoid when interacting with or supporting ISAOs?

As noted above, the United States government should take great care to ensure that it does not (and is not viewed to be) overshadow the framework for ISAOs or the standards that will be developed for them. ISAO formation should be truly organic, yet coordinated to ensure that existing ISAC and ISAO efforts are not duplicated. In addition, TIA urges for a neutral approach to be taken by DHS in its selection of the ISAO standards organization. For example, TIA believes that it would be inappropriate to select an organization representing a specific sector to develop best practices for all other sectors; rather, DHS is strongly advised to select an organization with adequate expertise and one that is widely supported across sectors.

In addition, TIA urges for the ISAO framework and ISAO best practices to reflect the priority for U.S.-based technologies' continued success in the global marketplace which has been enabled through the development of internationally-used standards and best practices. ISAOs should recognize that that the global nature of industries, such as the ICT industry, necessarily require a global approach to address cybersecurity concerns, and that a global supply chain can only be secured through an industry-driven adoption of best practices and global standards.

Further, the development of the ISAO concept and ISAO best practices should be cognizant of other Federal efforts that present the possibility of running in parallel to those of DHS in the cybersecurity information sharing space. For example, the FCC CSRIC's recently re-chartered efforts include several cybersecurity-themed and industry-led efforts, including a dedicated effort to address "cybersecurity information sharing,"[9] and the relationship between the DHS ISAO effort and that of the FCC CSRIC remains unclear. Absent constant and close coordination with other Federal efforts in the context of cybersecurity information sharing, the development of ISAOs may be disadvantaged, particularly for organizations with limited resources that may not be able to dedicate personnel to multiple fora at the same time.

Lastly, the Unites States government should also consider what incentives it can provide to organizations to form and/or participate in an ISAO that do not replicate existing ISACs. It remains unclear how the hundreds of ISAOs that DHS contemplates forming in the next few years will be funded initially, or how they will sustain funding. Further, it remains unclear how the participation of small and medium businesses can be maximized.

G. Question 7. Identify potential conflicts with existing laws, authorities that may inhibit organizations from participating in ISAOs and describe potential remedies to these conflicts.

Initially, TIA notes that it has long held that businesses of all kinds need practical liability safeguards to increase their cybersecurity threat information sharing capabilities. Despite the volume and complexity of cyber-based attacks increasing, without these assurances, many businesses will find themselves in uncertain legal terrain when contemplating sharing timely cybersecurity threat indicators and defensive measures that may be interpreted to put the well-intentioned sharing organization. No segment of the economy knows this better than ICT manufacturers, vendors, and suppliers; not only do TIA members themselves face constant cyber-based threats, but many also provide managed security services to telecommunications service providers and others, making contractual obligations with customers a concern. With

[9] *See* Agenda – June 24, 2015 FCC CSRIC V Meeting *at* https://transition.fcc.gov/bureaus/pshs/advisory/csric5/Agenda_CSRICV_06242015.pdf (last accessed July 7, 2015).

uncertainty as to whether the sharing of this key information – whether originating within the company or gained in the providing of a managed security service – the timely sharing of needed information will be slowed or prevented. For these reasons, TIA has supported Congressional efforts to improve this situation through bills including the Cybersecurity Information Sharing Act of 2015 ("CISA"). CISA's tailored protections in the areas of limited liability, disclosure, and antitrust would provide much-needed certainty that would encourage businesses' sharing of cyber threat data and defensive measures more quickly and frequently. Due to other sector-specific legal and regulatory requirements that exist domestically, ISAO standards should consider all existing laws that directly prohibit the sharing of consumer data.

Furthermore, recognizing that the global nature of the ICT industry necessarily requires a global approach to address cybersecurity concerns as described above, ISAO participation may be hampered by the growing body of legal and regulatory regimes internationally which address data protection in numerous contexts as well as the sharing of personally identifiable information. TIA continues to advocate globally for a harmonized, voluntary, and international standards-based approach to securing cyberspace, but faces threats in many key markets where governments continue to propose and adopt mandatory, inflexible, and enforcement-based approaches to cyberspace security. Neither ISAOs nor any other government action should implement cybersecurity policies that would restrict trade with other countries that are part of the global trading system. TIA believes that the ISAO framework and related standards contemplate their international impact, and move deliberately to ensure that impacts in an international context do not impact trade in a negative way.

H. Question 8. Please identify other potential challenges and issues that you believe may affect the development and maturation of effective ISAOs.

N/A – please see above.

II. CONCLUSION

TIA appreciates DHS' consultation regarding ISAOs, and urges consideration of the recommendations above. We stand ready to work with DHS and all other stakeholders towards improving cyber safety by augmenting information sharing capabilities, as well as through other means.

/s/

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Brian Scarpelli
Director, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 North Courthouse Rd.
Suite 200
Arlington, VA 22201
(703) 907-7700

July 10, 2015