June 17, 2016

Greg White
Executive Director
ISAO Standards Organization

Re: Docket No. DHS-2015-0017

Dear Dr. White:

NTCA–The Rural Broadband Association (NTCA) submits the following comments with regard to the preliminary drafts released last month by the Information Sharing and Analysis (ISAO) Standards Organization (SO). Before offering its comments, NTCA would like to recognize the substantial contributions of the Standards Working Group (SWG) leads and members that have supported the development of the preliminary drafts. The association appreciates that SWG members serve in a volunteer capacity and have graciously offered their time and knowledge to this important project.

Further, as you may know, the IT-Information Sharing and Analysis Center, the IT-Sector Coordinating Council, the Communications-Information Sharing and Analysis Center, and the Communications-Sector Coordinating Council recently submitted joint comments in regard to the preliminary SO drafts. NTCA strongly supports the feedback the IT and Communications sectors collectively provided, and it does not intend to rehash the suggestions in detail, but rather provide a companion document that highlights the unique challenges and needs of small communications providers, and offers targeted edits for various SWGs.

As a way of providing context to its recommendations, NTCA represents nearly 900 small, independent telecommunications providers. NTCA's members operate in the most sparsely populated and highest-cost rural areas of the country. In the face of substantial economic and geographic challenges, all of NTCA's members are full-service voice and broadband providers, and many also provide wireless, satellite, video, and/or other competitive services. The services they provide help put rural Americans on an equal footing with their urban neighbors. Rural providers are a critical link in the nation's telecommunications network, serving 40% of America's landmass, but less than 5% of the population. On average, an NTCA member company's customer density is approximately seven customers per square mile; by contrast, larger telecom companies serve, on average, 130 customers per square mile. NTCA's members also vary tremendously in size; however, the average company employs 27 staff, and has annual revenue of between $1 million and $5 million.

Although NTCA's members have more limited financial, technical, and personnel resources than their larger peers, they are no less committed to operating advanced and secure networks. Cyber-threat intelligence is a critical input into service providers' cybersecurity risk management plans. However, not all communications companies have the resources to participate within the existing Information Sharing and Analysis Center (ISAC) structure; rather, some small telecommunications providers may find that an alternative cyber-threat information sharing strategy better meets their needs.

As such, NTCA appreciates the Administration's efforts to create a "more flexible approach to self-organized information sharing activities amongst communities of interest such as small businesses across sectors…."[1] ISAOs may be "organized on the basis of sector, sub-sector, region, or any other affinity" and may be formed as

[1] *Frequently Asked Questions about ISAOs*, Department of Homeland Security, https://www.dhs.gov/isao-faq.

for-profit or non-profit entities.[2] Further, as the SO notes, "Some ISAOs may be formed on a very informal basis and may have little to no desire to collect and analyze information in near real-time for its members,"[3] while others may desire to offer near real-time information analysis and dissemination and/or other advanced capabilities. However, "[t]he goal of an ISAO SO is to be as inclusive as possible in finding a place for any individual or organization that wishes to be part of the Nation's overall information sharing effort."[4]

Small businesses will need inherent flexibility in regard to a new ISAO structure, and it is important to keep this primary tenet – flexibility – at the forefront as the SWG drafts are created. The resultant documents should refrain from creating a one-size-fits-all model, or a prescriptive list of mandated requirements that deter or even preclude participation in ISAOs by small businesses.

According to Executive Order 13691: *Promoting Private Sector Cybersecurity Information Sharing* (Executive Order) the mission of the SO is to develop "baseline capabilities that ISAOs under this order should possess and be able to demonstrate."[5] It is noteworthy that the Executive Order specifically uses the term *baseline capabilities*. Organizations will need fundamental guidance with respect to setting up an ISAO's operations. It is important to highlight that focusing on baseline concepts does not restrict or inhibit the growth of an ISAO; rather it provides an important foundation, which can be built upon by ISAOs that wish to develop or evolve their capabilities. However, similar to the NIST Cybersecurity Framework, not all industry participants will desire to offer mature capabilities and services at the forefront of the ISAO's inception.

The draft provided by SWG2, ISAO Capabilities and Categories, embodies this spirit, by providing a menu or "'shopping list' of capabilities"[6] organizations can pick and choose from to meet the needs of their respective members. SWG2 has met the primary needs of emerging ISAOs while also providing a path forward for more mature organizations, ensuring flexibility for all interested and participating organizations.

With these tenets in mind, NTCA urges the SWG leads to revisit the preliminary drafts, and, in particular, (1) the ISAO SO Product Outline, (2) Startup Topics (SWG1), and (3) Cybersecurity-Related Information Sharing Guidelines (SWG3) drafts.

1. For instance, within the ISAO Product Outline:
    - Line 125: The draft introduces the concept of a "fully capable" ISAO that "will provide a variety of services to support its members."[7] The term "fully capable" implies that an ISAO must meet a minimum level of service, especially when paired with a discussion of ISAO and organizational responsibilities concerning *Situational Awareness*, *Decision-Making,* and *Actions*. The items discussed under these subject headings extend far beyond the fundamental responsibilities of an ISAO enumerated within the Executive Order.

      For example, under the subject heading *Situational Awareness*, the drafts states that "ISAO members need to understand both the tactical and strategic aspects of the environment in which

---

[2] *Executive Order 13691: Promoting Private Sector Cybersecurity Information Sharing*, Section 3, https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari (Executive Order).
[3] ISAO SO Product Outline, lines 44-46.
[4] *Id*., lines 59-61.
[5] *Executive Order*.
[6] ISAO Capabilities and Categories (SWG2), line 12.
[7] ISAO SO Product Outline, line 130.

they are managing risks."[8] However, the Executive Order does not contemplate any new risk management responsibilities for ISAO members. Similarly, under *Decision-Making*, the draft states that "ISAOs need to disseminate actionable information that will enable their members to make decisions related to their security posture and allocation of security and IT resources."[9] However, the Executive Order does not state that the info produced and disseminated by an ISAO should be required to facilitate individual member investment decisions. And finally, under *Actions*, the draft states that "Organizations will develop detailed actions and assign responsibilities, implement the actions, and evaluate their effectiveness, providing feedback for their consideration." However, once again, the Executive Order did not mandate that individual organizations take any actions based upon ISAO-shared cyber threat info.

Not all ISAOs may desire to provide all such services and perform all such functions; rather an ISAO may simply wish to provide a "standard method to send and receive cyber threat indicators, vetting members (a trust capability), and storing threat indicator information…"[10] and those basic capabilities should be sufficient. By contrast, the additional concepts introduced by SWG1 such as those noted above create lofty minimum standards of service for an ISAO, which may be difficult to obtain and will likely artificially and unnecessarily deter smaller organizations and small businesses from participating within the ISAO model. Layering on such requirements would thus defeat, rather than promote, the information-sharing goals of the Executive Order.

- Line 183: The draft introduces the concept of ISAO certification. NTCA urges the SWGs to refrain from discussing certification standards at this early stage in development. Certification, particularly if tethered to specific, inflexible standards such as those described above, may yet again serve to deter participation from smaller, more resource-constrained organizations. Further, as noted by the Communications and IT Sectors, if there is going to be a certification developed, it should be voluntary, high-level, and private-sector driven. Certification should only serve a fundamental, basic purpose of ensuring organizations self-identify as an ISAO and express a commitment to information sharing and analysis.
- Lines 191-200: The draft includes a lengthy list of ISAO service offerings. However, many of the concepts proposed in the Product Outline stretch far beyond an ISAO's basic, foundational capabilities of collecting, analyzing, and disseminating threat information, as defined in the enabling Executive Order. For instance, a newly formed ISAO should not be expected to create a best practice library (line 193) or offer risk management support (line 198).

2. The ISAO Startup Topics (SWG1) includes a similar discussion of a "fully capable ISAO" (lines 106-112), which needs to be addressed and revised as noted above. Further, from a macro perspective, the document includes a list of Startup Topics (lines 104-536). At its core, this approach could be helpful. However, it reads as a prescriptive, inclusive list of requirements that an ISAO must have within its enabling structure, and the current list of topics infers that an organization must possess a level of maturity within its operations. Many of the items introduced within the Startup Topics list are not vitally necessary for an emerging ISAO. For instance, the draft includes a line of questions about the ISAO's board of directors' and officers' responsibilities, in addition to financial management, but leaves out the most important initial questions, such as "does my ISAO require a new board of directors?", and "does my ISAO require member dues to be collected?" Rather, the list of startup topics should be just that –

[8] *Id.*, lines 135-138.
[9] *Id.*, lines 139-141.
[10] ISAO Capabilities and Categories (SWG2), lines 25-26.

basic, fundamental questions an organization(s) should consider as it contemplates establishing ISAO operations in order to formally share and analyze cyber threat information. NTCA urges SWG1 to revisit the Startup Topic list with an eye toward flexibility, ensuring that the smallest organization(s) with limited resources and foundational information sharing needs can still participate.

3. Cybersecurity-Related Information Sharing Guidelines (SWG3): This draft opens by stating that "ISAOs need to be able to share information related to cybersecurity risks and incidents and collaborate…" Further, the executive summary states, "not all ISAOs may be capable initially or desire to fully achieve these objectives." Unfortunately, the draft perpetuates the use of the *Situational Awareness*, *Decision-Making*, and *Action* responsibilities, which, once again, extend far beyond the basic capabilities and requirements of an ISAO. Further, it quickly divulges into a complicated discussion of advanced ISAO capabilities, such as response measures, coordination, and trend and pattern analysis. NTCA urges SWG3 to revisit the document, developing fundamental guidelines for how cyber-threat info can be shared in its most basic format and using a simple mechanism, and then provide guidance on how an ISAO can evolve and progress its offerings. The draft should clearly differentiate between primary info sharing guidelines, and advanced capabilities of more mature organizations.

Thank you in advance for your consideration and review. NTCA looks forward to further engaging with the ISAO SO and the SWGs in regard to refining the draft standards.

Regards,

/s/Jesse Ward
Jesse Ward
Industry & Policy Analysis Manager
NTCA–The Rural Broadband Association
703-351-2007
jward@ntca.org

/s/ Jill Canfield
Jill Canfield
Vice President and Assistant General Counsel
NTCA–The Rural Broadband Association
703-351-2020
jcanfield@ntca.org