NTCA THE RURAL BROADBAND ASSOCIATION

August 5, 2016

Greg White
Executive Director
ISAO Standards Organization

Re: ISAO 100-1 *Guidelines for Establishing an ISAO* v0.1; and ISAO 600-1 *U.S. Government Relations* v0.4

Dear Dr. White:

NTCA–The Rural Broadband Association (NTCA) submits the following comments with regard to the Information Sharing and Analysis Organization (ISAO) 100-1 *Guidelines for Establishing an ISAO* v0.1, released on July 22, 2016, and ISAO 600-1 *U.S. Government Relations* v0.4 released on July 27, 2016. Before offering its comments, NTCA would like to recognize the substantial contributions of the Standards Working Group leads and general members that have supported the development of the draft guidelines.

Unfortunately, NTCA remains concerned about the overall direction of the ISAO Standards Organization (SO) work products. *Executive Order 13691–Promoting Private Sector Cybersecurity Information Sharing* stresses the development of an inclusive ISAO structure that is flexible and scalable for organizations of all sizes and resources; these primary, guiding tenets are further recognized within the 100-1 v0.1 draft, Section 2: Introduction, and Section 4: What is an ISAO?. However, later portions of the draft depart from these core principles. As such, NTCA urges the SO to revisit the draft guidelines with an eye toward flexibility and scalability for all interested participants as contemplated by the guiding tenets of this process.

More specifically, NTCA urges the SO to refrain from creating guidelines that are overly prescriptive and burdensome. For instance, the SO has discussed the development of lofty minimum requirements for ISAOs, which would be enforced though a third-party certification model. This approach would reduce the operational viability of the ISAO model for small businesses. A third-party certification regime also would be inconsistent with Executive Order 13691, which provided the legal basis and direction for the ISAO initiative and did not contemplate the use of a certification as a requirement for voluntary ISAO participation. Finally, within ISAO 600-1, the SO should include the Federal Communications Commission (FCC) Communications, Security, Reliability and Interoperability Council's (CSRIC) *Cybersecurity Risk Management and Best Practices Working Group 4: Final Report*,[1] which provides substantive guidance to communications carriers in regard to how to use the *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0* (the NIST Cybersecurity Framework) to identify, protect, detect, respond, and recover from a cyber attack.

To provide context for these 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, NTCA's members are full-service voice and broadband providers, and many also provide wireless, satellite, video, cloud computing, and/or other competitive services. Rural providers are a critical link in the nation's telecommunications network,

[1] Federal Communications Commission (FCC) Communications, Security, Reliability and Interoperability Council's (CSRIC) *Cybersecurity Risk Management and Best Practices Working Group 4: Final Report*, rel. March 2015, https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

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 fewer financial resources and personnel than their larger peers, they are no less committed to operating advanced and secure telecommunications networks and no less interested in protecting those networks and their users. Cyber-threat intelligence can be 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.

Of import, rural telecommunications providers have existing, trusted relationships with their industry peers and across sector lines. As community-based companies, the employees of the local, rural telecommunications provider, including the senior executives, reside within the community where they operate. Likewise, the rural electric provider and rural water system often employ individuals from the local community. Given this small-town atmosphere, executives of these critical infrastructure providers may have established, trusted relationships. Further, serving more sparsely populated areas, NTCA's members often share a like-minded independent spirit, and face similar challenges in operating in rural areas. As such, it is common for rural telco executives and technicians to collaborate with their peers at other companies – whether that is the neighboring independent telecommunications providers, or a similarly situated telco across state or regional boundaries.

Given this background, 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…."[2] ISAOs may be "organized on the basis of sector, sub-sector, region, or any other affinity" and may be formed as for-profit or non-profit entities.[3] "There will be "varying levels of organizations"[4] within ISAOs, and "[s]ome 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*,"[5] 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."[6]

Further, according to Executive Order 13691, the mission of the SO is to develop "baseline capabilities that ISAOs under this order should possess and be able to demonstrate."[7] It is noteworthy that the Executive Order specifically uses the term *baseline capabilities*. Organizations will need and welcome fundamental guidance with respect to setting up an ISAO's operations. But they require guidance rather than prescription – they need to know what "baseline capabilities" are important in providing a foundation for information sharing. 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. Instead, it is quite accurate to say, as the draft

[2] *Frequently Asked Questions about ISAOs*, Department of Homeland Security, https://www.dhs.gov/isao-faq.
[3] Executive Order 13691, Section 3, https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari (Executive Order 13691); ISAO 100-1 *Guidelines for Establishing an ISAO* v0.1, rel. July 22, 2016, Section 2: Introduction, lines 21-22 (ISAO 100-1 v0.1).
[4] ISAO 100-1 v0.1, Section 2: Introduction, line 38.
[5] *Id.*, lines 39-41 (emphasis added).
[6] *Id.*, lines 54-56.
[7] Executive Order 13691, Section 3.

rightly recognizes in other parts, that some ISAOs will "be formed on a very informal basis" for the purposes of permitting and promoting sharing among entities that might otherwise not do so.

Once again, NTCA urges the SO to review the current ISAO 100-1 v0.1 draft with these precepts in mind. The SO 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. Further, consistent with these macro recommendations, the association offers the following specific feedback in regard to ISAO 100-1 v0.1 and ISAO 600-1 v0.4:

1. ISAO 100-1, Section 5.1: Introduction to Capabilities is inconsistent with Executive Order 13691 in that it professes that ISAOs offer mature capabilities that extend far beyond the precepts of cyber threat information sharing and analysis. ISAO 100-1, Section 5.1 should be revised to ensure it is consistent with the language and concepts introduced in ISAO 100-1, Section 5.5: Describing ISAO Capabilities, i.e. *foundational*, *additional*, and *unique capabilities* of ISAOs.
   - Section 5.1 introduces the concept of a "fully capable"[8] ISAO that "will provide a variety of services to support its members."[9] 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 Executive Order 13691.
   - 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 they are managing risks."[10] However, Executive Order 13691 does not contemplate any new risk management responsibilities for ISAO members. Similarly, under *Decision-Making*, the draft states, "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."[11] 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: "Organizations will develop detailed actions and assign responsibilities, implement the actions, and evaluate their effectiveness, providing feedback for their consideration."[12] However, once again, Executive Order 13691 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…"[13] and those baseline capabilities should be sufficient. By contrast, the additional concepts introduced by Section 5.1 such as those noted above create lofty, minimum standards of service for an ISAO, which may be difficult to obtain, and may 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 Executive Order 13691.

[8] ISAO 100-1 v0.1, Section 5.1: Introduction to Capabilities, line 124.

[9] *Id.*, line 128.

[10] *Id.*, lines 133-134.

[11] *Id.*, lines 137-139.

[12] *Id.*, lines 144-146.

[13] ISAO 100-1 v0.1, Section 5.5: Describing ISAO Capabilities, lines 853-855.

- The SO should review ISAO 100-1, Section 5.1 to ensure it is flexible and scalable for organizations of all sizes. Further, ISAO 100-1, Section 5.5 provides clear and consistent language that should be adopted throughout the 100-1 document. Section 5.5: Describing ISAO Capabilities introduces the concepts of *foundational*, *additional*, and *unique capabilities*, which provides a starting point for emerging ISAOs and a path to maturity for those who desire to become more sophisticated.[14] "There is no requirement to 'package' or select any specific capability or groups of capabilities – it is a pick-and-choose environment."[15]

2. Similarly, ISAO 100-1, Section 5.2: Value Proposition affirmatively asserts that ISAOs will provide their members with a lofty list of benefits that countermands the flexibility and scalability called for in Executive Order 13691. For instance, Section 5.2 states, "[a]n informative set of cybersecurity threat indicators and best practices provided by ISAOS will make individual members more secure", and "[m]embers enhance their knowledge about how to protect themselves from, detect, and react to cyber attacks." Although these are admirable goals, not all ISAOs will possess the maturity of operations required to deliver these capabilities. For instance, many emerging ISAOs will be unable to provide best practices or mitigation techniques, and/or promise that members will be more secure by participating within the ISAO structure. Section 5.2 should be revised to ensure that it incorporates emerging, foundational capabilities and benefits to members, as described in Section 5.5 and consistent with the Executive Order 13691.

3. ISAO 100-1, Section 5.4.3: ISAO Membership, Section 5.4.4: ISAO Marketing and Communications, and Section 5.4.5: ISAO Operations and Financial Management, should also be reviewed with an eye toward flexibility and scalability. These sections should enumerate the operational components that ISAOs may wish to consider as they formalize their operations. However, rather than options to consider, these sections read as prescriptive, inclusive requirements that an ISAO must achieve, and many of the items introduced within these sections are not vitally necessary for an emerging ISAO that offers foundational capabilities. For instance, Section 5.4.3 states, "ISAO membership includes establishing a membership model consisting of ...the cost to join the ISAO"[16]. Section 5.4.4 states that an ISAO "should define and have resources to implement a marketing and communications strategy"[17], and then enumerates specifics and tactics of the strategy. However, it leaves out the most important initial questions, such as, "Does my ISAO require member dues to be collected?" and, "Is a sophisticated member communications strategy necessary to meet the needs of my members and the ISAO?" As an alterative, these sections should provide basic, fundamental questions an organization(s) should consider as it contemplates establishing an ISAO in order to formally share and analyze cyber threat information. The SO should revisit Sections 5.4.3, 5.4.4, and 5.4.5 with an eye toward flexibility, ensuring that the smallest organization(s) with limited resources and baseline information sharing needs can still participate.

4. Although not specifically discussed within the ISAO 100-1 v0.1 draft, NTCA understands that the SO is considering the concept of third-party certification, wherein a company or contractor would evaluate whether an organization(s) meets a set of pre-defined, minimum criteria in order to obtain the ISAO brand. However, 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, the concept of third-party certification was never discussed within the presiding

[14] *Id.*, lines 842-884.
[15] *Id.*, lines 880-881.
[16] ISAO 100-1 v0.1, Section 5.4.3: ISAO Membership, lines 448-449, and 456.
[17] ISAO 100-1 v0.1, Section 5.4.4: ISAO Marketing and Communications, lines 482-484.

Executive Order 13691. As such, if there is going to be an ISAO 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 cyber threat information sharing and analysis.

5. Finally, turning to ISAO 600-1 v0.4, the SO should include the FCC CSRIC *Cybersecurity Risk Management and Best Practices Working Group 4: Final Report*[18] among its many listed resources. The report provides substantive guidance for communications carriers in regard to how to use NIST Cybersecurity Framework to identify, protect, detect, respond, and recover from a cyber attack. More than 100 industry experts participated in the working group 4 effort, representing all facets of the communications sector. The final report provides detailed, scalable guidance to protect an operator's core network and critical infrastructure.

In summary, NTCA urges the SO to revisit the ISAO 100-1 v0.1 draft with an eye toward flexibility and scalability to ensure that small businesses can and will participate in the ISAO effort. The SO should refrain from driving toward an end product that is overly prescriptive. The SO should also include the FCC CSRIC report as a resource within the ISAO 600-1 document.

Thank you in advance for your consideration and review. NTCA looks forward to further engaging with the ISAO SO 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/ Michael Romano
Michael Romano
Senior Vice President, Industry Affairs &
Business Development
NTCA–The Rural Broadband Association
703-351-2016
mromano@ntca.org

[18] Federal Communications Commission (FCC) Communications, Security, Reliability and Interoperability Council's (CSRIC) *Cybersecurity Risk Management and Best Practices Working Group 4: Final Report*, rel. March 2015, https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.