January 14, 2018

Greg White
Executive Director
ISAO Standards Organization

Re: *Solicitation for Discussion on an ISAO Certification Model*

Dear Dr. White:

NTCA–The Rural Broadband Association (NTCA) submits the following comments regarding *Solicitation for Discussion on an ISAO Certification Model*, released on December 1, 2017.[1]

NTCA recognizes and appreciates the important contribution the Information Sharing and Analysis Organization (ISAO) Standards Organization (SO) has made to our nation's security. Our collective cybersecurity posture is strengthened as businesses build and evolve their cyber risk management programs, and cyber-threat intelligence can be important input into an organization's risk management plan. Indeed, many of NTCA's members are important stakeholders in the ISAO standards development process.

However, the current SO proposal to require a certification regime for ISAOs will have the unintended impact of making it harder for NTCA's members to create an information sharing community that meets their needs. An ISAO certification regime is at best premature, and it may (albeit inadvertently) increase the barriers to entry and thereby deter participation in the ISAO development process from small businesses – an important and perhaps vital population that *Executive Order 13691–Promoting Private Sector Cybersecurity Information Sharing*[2] sought to engage in the nation's information sharing ecosystem. Given these concerns, NTCA urges the SO to retreat from any certification approach, including a self- and/or third-party certification model.

NTCA represents more than 850 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, serving 37% of America's landmass, but less than 5% of the nation's population. NTCA's members vary tremendously in size; however, all of NTCA's members are small businesses. 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. 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 such, it is common for rural telco executives and technicians to collaborate with their peers – whether that is the neighboring independent telecommunications providers, or a similarly situated telco across state or regional boundaries. As such, many of NTCA's members are vital constituents in the ISAO standards development process, as they are active and/or interested participants in the ISAO community.

[1] *Solicitation for Discussion on an ISAO Certification Model*, Request for Comment: Open December 1 – January 15: https://www.isao.org/drafts/solicitation-for-a-discussion-on-an-isao-certification-model/.
[2] *Executive Order 13691–Promoting Private Sector Cybersecurity Information Sharing*, rel. Feb. 13, 2015: https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

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…."[3] 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.[4] Accordingly, "ISAOs will vary in terms of size, objectives, and capabilities."[5] Given this foundational direction, flexibility and scalability should be inherent in the ISAO guideline development process.

In its written proposal and public statements, the SO repeatedly cites trust and the development of trust as the underlying need for its certification proposal. However, the SO mistakenly equates certification with trust, implying that an ISAO certification will create and/or strengthen the trust between an ISAO's members and/or between an ISAO and the larger security community. Rather, an ISAO is formed to meet the needs of its members, and it is only successful if the ISAO establishes and nurtures a trusted bond among its membership and with other organizations. Further, the term ISAO itself has, at best, limited meaning outside the Washington, D.C., beltway[6]; certification to the SO's standards would, likewise, have minimal or no relevance to an ISAO's participants. Confidence in an ISAO's organization is created by continually meeting members' needs and capabilities over time, not via external certification. Indeed, *ISAO 100-1: Introduction to ISAOs* states, "ISAOs help establish and maintain trust relations among members by establishing a framework of common, shared values and expectations."[7] Likewise, regarding trust and sharing of info *between* various ISAOs, organizations will not share amongst themselves unless trust is present, and certification cannot replace the trusted bond and/or contractual arrangement required to necessitate the free flow of information sharing.

Further, a certification regime only serves to increase an ISAO's complexity and cost. Creating an ISAO is already a daunting undertaking – organizing members, formulating a governance structure, and establishing a funding mechanism are just a few of the foundational and monumental tasks required to build an ISAO. Certification, even self-certification, will require an ISAO to allocate its extremely limited financial and operational resources to demonstrate to external stakeholders that it is meeting external standards derived by the SO – resources that would be better suited to meeting members' needs. By increasing the barriers to entry to the ISAO ecosystem, the SO may (albeit inadvertently) deter participation from smaller and more resource-constrained organizations.

A certification approach also contradicts 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 a *voluntary* ISAO construct. Executive Order 13691 stresses the development of an inclusive, voluntary ISAO structure that is flexible and scalable for organizations of all sizes and resources. "The goal of the ISAO SO is to be as inclusive as possible in finding a place for an individual or organization wishing to be part of the overall information sharing effort."[8] However, as discussed above, unfortunately a certification regime may artificially discourage and thereby restrict participation.

As to the specifics of the proposal, the SO suggests certification to minimum service standards, as defined by *ISAO 100-2: Guidelines for Establishing an Information Sharing and Analysis Organization*, and *ISAO 200-1: Foundational Services and Capabilities*.[9] However, 100-2 correctly provides flexibility and scalability, consistent with the underlying EO, allowing for different types of ISAOs based upon member needs. In fact, 100-2 "offers guidelines for ISAOs to consider as they design and implement a collection of services and capabilities to meet the needs of their members," and it provides an "illustrative list of services and capabilities."[10] Further, 100-2 explicitly states that an ISAO "does not need to provide

---

[3] *Frequently Asked Questions about ISAOs*, Department of Homeland Security, https://www.dhs.gov/isao-faq.
[4] *Executive Order 13691*, Section 3; *ISAO 100-1: Introduction to ISAOs*: https://www.isao.org/wp-content/uploads/2016/10/ISAO-100-1-Introduction-to-ISAO-v1-01_Final.pdf, Section 2: Introduction.
[5] *ISAO 100-1*, Section 2: Introduction.
[6] At the International Information Sharing Conference 2017, a representative from the SMB ISAO noted in her presentation that she does not use the term "ISAO" with potential or current members, as it does not have any meaning outside the Washington, D.C., community.
[7] *ISAO 100-1*, Section 4: Value Proposition.
[8] *Id.*
[9] *Solicitation for Discussion on an ISAO Certification Model*, Lines 27-28.
[10] *ISAO 100-2: Guidelines for Establishing an Information Sharing and Analysis Organization*, v*1.01*, https://www.isao.org/wp-content/uploads/2016/10/ISAO-100-2-Guidelines-for-Establishing-an-ISAO-v1-01_Final.pdf, rel. Oct. 14, 2016, Section 3.5.

all of the foundational services or capabilities enumerated hereafter to be considered an ISAO."[11] As such, from a practical standpoint, creating a certification regime around a set of flexible and non-prescriptive guidelines would be quite difficult.

As to the second document, 200-1 is currently in draft form and consensus has not yet been reached on this document. Indeed, under separate cover NTCA raised concerns with the draft guideline.[12] As previously stated, the draft of 200-1 extends far beyond its mission as stated – "a comprehensive overview of the *foundational* services and capabilities of an ISAO."[13] Rather, the draft of 200-1 highlights various capabilities that infer a level of sophistication that may not be present, required, or even desired by an ISAO in a foundational stage of development, and further implies that ISAOs need to be formal groups with established governance structures. The 200-1 v0.1 foundational capabilities draft is increasingly problematic when it may serve as a guideline for certification. By enacting a certification regime that is thereby tied to lofty minimum requirements, the SO would, as previously discussed, dramatically increase the barriers to entry and participation, thereby reducing the operational viability of the ISAO model for smaller organizations.

Finally, and perhaps most importantly, the SO's current certification proposal is neither consensus-based nor community-driven. The concept of certification was discussed at length back in the Fall of 2016, when the initial set of ISAO guidance documents were crafted. At that time, a certification proposal was highly controversial and ultimately rejected by stakeholders at the SO's September 1, 2016, meeting. NTCA's concerns have not changed and the association urges the SO to consider the repercussions on the emerging ISAO community.

Once again, NTCA urges the SO to revisit its commitment to a certification regime. Given the importance of cyber-threat information sharing to the larger cybersecurity ecosystem, the SO should encourage and nurture participation in the ISAO model from all interested stakeholders. However, despite the association's concerns, if the SO decides to proceed forward, NTCA also offers an alternative proposal; at a minimum, if the SO determines that it must create an ISAO certification regime, 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.

Thank you in advance for your consideration and review. NTCA looks forward to further engaging with the SO as it seeks to refine the draft standards.

Regards,

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

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

[11] *ISAO 100-2*, Appendix A.
[12] See NTCA comments on *ISAO 200-1 v0.1* submitted Nov. 30, 2017.
[13] *ISAO 200-1*: *Foundational Services and Capabilities v0.1*, *Draft,* rel. Oct. 30, 2017, https://www.isao.org/wp-content/uploads/2017/11/ISAO-200-1-Draft-Foundational-Services-and-Capabilties-v01.pdf, Line 22 (emphasis added).