Name: Ola Sage

Email: osage@e-mcinc.com

Comments:

Dear Dr. White:
Since our establishment in 2006, the Information Technology Sector Coordinating Council (IT SCC) has been designated under the National Infrastructure Protection Plan to serve as the principal entity for coordinating with the government on a wide range of critical infrastructure protection and cybersecurity activities and issues. The IT SCC brings together companies, associations, and other key IT sector participants to work collaboratively with the Department of Homeland Security other government agencies, and other partners. Through this collaboration, the IT SCC works to facilitate a secure, resilient, and protected global information infrastructure. Our decade plus long involvement in promoting effective cyber policy, including information sharing, provides us with a unique and impartial perspective.
The IT SCC and our members have been actively engaged in the work of the Standards Organization (SO). Our members are committed to cybersecurity and, as such, many of our members participate in at least one information sharing organization. We continue to engage in this topic since we have long considered it to be a priority for the country to build and maintain effective and efficient mechanisms for the sharing and analysis of cyber threat information. The IT SCC offers these comments on the Standard Organization's proposed certification program. The Information Technology Sector Coordinating Council encourages the Standards Organization to reconsider its certification proposal and urges it to instead focus on community led, consensus driven initiatives that brings established and emerging organizations together to address common issues in a collaborative way. The Standards Organization's role as an impartial facilitator is important as the market for ISAO's takes shape. We share the Standards Organization's goal of building trust within an information sharing community and across organizations. However, we do not agree with the Standard Organization's assessment that a certification program is required to build trust. The experience of the IT-ISAC, which has been facilitating cyber threat information sharing within the IT Sector since 2001 and with other ISACs (and other partners) since 2003, and other information sharing forums demonstrates this point. Trusted interactions and information exchanges take place among noncertified organizations in the global marketplace each day.

The Standards Organization and others have justified certifications as a means of creating or managing a market for ISAOs. This betrays a fundamental misunderstanding of market economics in the digital age. Certification programs, by definition, limit options to fulfill user needs. If the digital economy demonstrates anything it is that it is unfettered innovation that expands options and improves consumer benefit. For example, we did not need a certification program defining social media to create Facebook or Twitter. Uber was created expressly by disrupting the certification program (taxi medallions etc.) that had been implemented to define and limit consumer options for car services.
Instead, we believe the single most effective mechanism for maintaining and enforcing trust relationships and growing the number of information sharing organizations is the market. If an organization does not provide effective services or operates in an untrustworthy manner, other

actors in the marketplace will not transact with that organization. Markets, as opposed to regulations, are especially effective when sharing across the global stage where even a hint of geopolitics can interfere.

A certification program for ISAOs at this stage is at best premature and most likely will be counter-productive to the stated goal of the Presidential Executive Order 13691, which is to expand options for information sharing. For example, a certification program will create unnecessary barriers for the creation of new ISAOs and perpetuate the false notion that an ISAO must do certain things in a certain way to be successful. The IT SCC objected to a previous effort to create a "model ISAO" for this reason. Our members are similarly concerned that a certification program places compliance over flexibility. Instead of being free to adapt to the needs of their member companies, information sharing organizations would be required to offer capabilities and services, and adhere to a business model that meets certification requirements. In contrast, to increase the number of newly formed ISAOs, the SO should minimize complexity and costs.

In fact, flexibility is embedded in the Standards Organization's own documentation. For example, ISAO 100-2 emphasizes on page 18 that an ISAO does not need to deploy any, let alone all, of the services and capabilities listed to be considered an ISAO. However, as detailed in the SO's certification proposal (lines 27, 44 and 47), the position of the Standards Organization is that an organization must possess or provide each of the "Foundational" services and capabilities to be considered an ISAO. The former is more closely aligned with the intent of the Executive Order. The Council is confused as to why the Standards Organization is taking a position that is clearly contrary to the content of its own community driven guidance.

While the Standard Organization's position is that this program would be a "voluntary," the SO does not have the authority to ensure that it remains voluntary. The SO cannot control how its certification program is used by government policy makers or regulators. Once the Standards Organization issues a certification program, it will create the perception that there are certain things an ISAO must do. This is likely to lead to mandatory compliance, which will require organizations to devote scarce resources to meeting compliance checklists rather than the needs of their members.

Adhering to a community driven, census based approach is paramount to reaching the stated goal of having hundreds or thousands of ISAO's in operation. Introducing a certification program as a foregone solution while challenging the community to convince the SO otherwise runs counter to the very trust the SO is tasked with facilitating. We urge the SO council to shepherd, rather than shape, the ISAO marketplace.

The primary objective of the SO ought to be assisting and guiding emerging information sharing organizations to share information that reduce cyber risk. Until the SO has defined and demonstrated that this objective has been achieved, a certification program is premature. A certification program should at best be a secondary development to be considered only after the guidelines the SO has created are shown to spur greater sharing of actionable information. A useful mechanism to address this required interim step between standards development and certification might be the NIST 1.1 process proposed in the current CSF proceeding.

As an alternative to a certification program, the Information Technology Sector Coordinating Council suggests the Standards Organization can better achieve its goals if the Standards Organization were to:

● Initiate a partner or mentor program, where it matches newly formed organizations with established organizations. This will help new ISAOs learn from and gain the trust of existing organizations and will help introduce existing organizations to newly established organizations.

● Host a workshop, or series of workshops, reserved for established and newly formed ISAOs as a means of introducing organizations to each other. The ability to meet and learn from each other could be invaluable and provide immediate dividends. Virtual workshops or webinars could be an acceptable alternative if an in-person workshop (or a series of in person workshops) is not practical.

● More actively promote and/or summarize the core components of trust contained throughout the SO documentation. If the goal is to increase trust, perhaps the SO can create a new document on the topic that pulls from existing guidance contained in the SO documentation and provides a couple examples on how to implement some of that guidance.

● Create a guide for companies considering joining an ISAO to help them evaluate which ISAO, if any, to join. This guide could help companies understand what their existing needs and capabilities are so that they can find an organization that can best meet their needs.

● Create a resource guide on the Standard Organization's website. While the Standards Organization currently lists "Registered" ISAOs on its website, this does little more than point website visitors to the home pages of each listed organization. Perhaps the SO can work with these organizations to provide more comprehensive information on the SO website about which of the services and capabilities the organizations provide.

● Expand Appendix A of ISAO 100-2 to include an index of where the services and capabilities are addressed in the SO documentation. This would make it easier for ISAOs to form and be effective by identifying where to find the information they need to implement the service or capability as needed and appropriate for their membership.

Finally, we must note the multiple conflicts of interest in the Standard Organization's proposal, which have been raised by others. The proposal establishes the Standards Organization as the initial certifying organization and then as the organization that will approve the certifying authorities. The quick pivot from the tax-payer supported standards development process into a money-making certification program with obvious links to the personnel involved in the government supported SO process will no doubt cause --- has already caused -- questions to be asked about conflicts of interest in the SO process. This can only undermine trust in the process in its entirety.

Given the relative infancy of the SO's work, the inability to measure how or whether organizations are implementing its guidance and the effect this guidance is having in improving security, it is premature to create a certification program. Since certification will impede innovation and market development and since there are several other more pragmatic steps to undertake at this stage, moving to a certification process at this time is both unwise and counterproductive. We respectfully urge the SO to reconsider its proposal.

Thank you very much for considering our comments.