January 15, 2018

Dr. Greg White
Executive Director, ISAO Standards Organization
Executive Director, Center for Infrastructure Assurance and Security
The University of Texas at San Antonio
Greg.White@utsa.edu

Allen Shreffler
Deputy Director, ISAO Standards Organization
Senior Cybersecurity Analyst, LMI
ashreffler@lmi.org

Rick Lipsey
Advisor, ISAO Standards Organization
Senior Strategic Cyber Lead, LMI
rlipsey@lmi.org

Subject: FS-ISAC's Response to Request for Comment on Proposed ISAO Standards Organization Certification Model

Dear Dr. White, Mr. Schreffler, and Mr. Lipsey:

FS-ISAC is one of the more visible cybersecurity information sharing organizations. We share the belief with the ISAO Standards Organization that information sharing should be broadly promoted and adopted across a variety of industries, segments, regions and use cases. At the same time, we believe that creating complexity and barriers to sharing can potentially discourage the overall ecosystem of sharing. FS-ISAC appreciates the opportunity to provide input on the proposed ISAO Certification model that has been presented for public comment.

The following is the FS-ISAC's comment to the ISAO Standards Organization proposal for ISAO certification.

FS-ISAC is strongly against ISAO certification for the following reasons:

- Trust must be earned, it cannot be mandated
- Certification places undue burden and barriers to sharing on fledgling ISAO, sharing groups & international sharing
- Sharing mechanisms are available today that work and do not require certification
- There is potential legal liability in the case of an attack or breach
- Certification can lead to unnecessary regulation

Our response below in part one explains the rationale behind our point of view. Part two of the comment letter relays some alternative approaches that could be helpful to the ISAO Standards Organization as it identifies next steps in the process.

Response Part One: Rationale Against Certification

The FS-ISAC does not support a formal "third party" certification as an approach to establish the "trust" needed for the robust interaction among ISAOs or an effective use of ISAO resources. Here are our reasons for not supporting certification.

- **Trust is earned, not certified.** Mutual trust between organizations is created through a progressive process where the quality of inter-organizational interactions, exchanges and relationships reinforce the reliability and confidence in cooperative efforts. While the ISAO Standards body envisions "hundreds or thousands" of sharing organizations, the fact is there are just a few ISAOs today and they should be established as individual markets, industries, segments and functional areas require them. FS-ISAC and other ISACs and ISAOs do not currently envision a future with "hundreds or thousands" of sharing organizations. In fact, since the Presidential Cybersecurity Information Sharing Act was signed years ago under President Obama, just a handful of ISAOs have been stood up, and ISAOs like the legal services ISAO (LS-ISAO) have been very effective without requiring certification and have even participated in robust cross sector sharing. Even if many more sharing organizations are created, sharing mechanisms already exist today including sharing agreements, information labeling (Traffic Light Protocol) and other mechanisms like "circles of trust" that lead to trusted sharing relationships.

- **Barrier to new sharing**. Certification presents a barrier to new sharing organizations including ISAOs which typically have very limited resources to get up and running. Certifications adds additional compliance costs and efforts for information sharing organizations that operate as lean non-profits and can detract from the mission of these organizations. It also presents a barrier to cross-sector sharing potentially. There is also a strong presence of technology vendors in the sharing ecosystem (for example a category known as Threat Intelligence Platforms or TIPs) which are innovating the way organizations share. Requiring these entities to certify would potentially inhibit the innovation and real-time data sharing that is enabled through these technologies.

- **Differing service levels & industry requirements.** ISAOs can choose to voluntarily self-declare the type of services they provide to their members, however different ISAOs will have very different service offerings and so trying to certify in an "apples to apples" way could be difficult if not impossible to do in a neutral and fair way. There is currently a conflict in the ISAO Standards Proposal regarding whether or not all services would have to be certified or not. This will lead to confusion amongst both sharing organizations, their members and their potential members. Organization will be more responsive to efforts which directly support their need for trusted relationships versus expending resources on some generic approach. In addition, when it comes to cross-sector sharing, certification could also be an issue. For example, the FS-ISAC works with other sectors including Retail, Oil and Gas, Legal Services and many others. The differences in information sharing needs across these sectors are staggering. While there are some shared common threats and vulnerabilities along the threat chain, the

differences are greater than the similarities. Each sector will need its own set of requirements and potentially its own set of certifications, leading to undue burden both to maintain these standards, certify to them and adhere to them.

- **A "solution in search of a problem."** Certification is not in use today despite dozens of sharing organizations including ISAOs, ISACs and technology-driven initiatives. Different levels of trusted relationships among sharing communities, including ISAOs, already exist and will continue to evolve and no broad standard approach will respond adequately to these needs. Where institutional trust is needed, mechanisms such as contracts and sharing agreements that are combined with observed continuous operational competence, performance and interactions provide a more concrete basis.

- **Global challenges abound.** Sharing today does not stop at borders. There is robust sharing across multiple countries and regions. Certification that takes this complex landscape into account would necessarily be extremely complex and add to the operational burdens already faced by ISAOs. Further, it is extremely pre-mature to pursue certification across international borders without an agreed upon U.S. approach and engagement of all U.S. stakeholders.

- **Certification can tip towards regulation & legal issues.** Many sectors, including the financial services sector are already heavily regulated. If ISAOs proceed down the slippery slope of certification, this could become *defacto* regulation or contribute strongly towards tipping to regulation. It's also important to note that certification could create potential legal liability in the event an ISAC or ISAO is breached/attacked.

Part Two: Alternative Recommended Approaches

FS-ISAC recommends that instead of expending energy on creating an unnecessary and burdensome certification process, that instead the ISAO SO survey the methods existing ISAO and ISAC have successfully used in establishing productive trust relationships among private sector entities and existing trusted relationship with public sector entities. Successful recent examples including the standing up of the Legal Services ISAO (LS-ISAO) which grew to over 100 members in just 12 months with extremely successful sharing practices, the standup of the Retail ISAO or R-CISC which did not require certification, and the creation of the Energy Analytic Security Exchange (EASE). These are just a few examples. The following are additional recommendations.

- **Strive for trust via existing trust mechanisms & relationships.** Instead of certification, advocate for trust via proven mechanisms. Examples include adoption of the Traffic Light Protocol, use of Circles of Trust and agreed information sharing mechanisms via public to private partnerships. The trust basis in these mechanisms is self-re-enforcing in 'real time' and so is a more potent way to ensure proper sharing between entities. Trust must be earned, not certified and not regulated. Existing ISACs

and ISAOs align themselves with partners including industry partners, solution providers, government entities, CERTS and other bodies. Rather than focusing on certification, rather developing best practices to recruit and maintain such relationships would be most beneficial to information sharing entities.

- **Create a "National Council of ISAOs".** Similar to the National Council of ISACs, this group requires an application process (not certification) and becomes part of a council with regular communications and regular meetings. This again enables peer to peer re-enforcement of sharing activities and practices. This group could also lead important education initiatives around sharing. For example, so that sharing does not 'tip' into regulation, educate regulators in each major sector regarding the importance of sharing and the importance of self-governance per region.

- **Standardize data, vet members.** Instead of focusing on standardizing and certifying the ISAOs themselves, focus on the data types and standards that are shared. For example, supporting STIX and TAXII as threat indicator sharing standards has been very important for existing ISACs and ISAOs. Likewise, the ISAO SO could guide sharing organizations in how to best vet new members joining the sharing organization. ISACs have an existing process for this and it helps ensure the integrity of the sharing membership in each organization.

- **Establish a scorecard.** Consider a scorecard approach reported on a regular basis per sharing entity. Rather than certification, this provides a more frequent and transparent basis for monitoring sharing practices and ensuring proper sharing. Instead of certification, recommend governance models and monitor which sharing organizations adopt proper governance. Add that to the scorecard.

- **Support cross sector & global sharing best practices.** Instead of a one time or even annual certification, instead research and publish best practices around cross-sector, ISAO to ISAO and ISAO to ISAC sharing practices. Certification is an inhibitor to global sharing. Instead, the ISAO Standards Organization should look to models already in existence for regional sharing initiatives and publish best practices relating to international and regional sharing. This could also be part of the scorecard and monitoring. Three often used mechanisms for sharing include the Traffic Light Protocol (TLP), establishing Circles of Trust, and templates for information sharing agreements between organizations. There are also models for cross sector sharing and cross border sharing in existence today.

In summary, for the reasons stated above and because there are existing practices and approaches that do not require certification, FS-ISAC does not support the ISAO certification approach. We do, however, support broad scale adoption of information sharing across industries, segments, regions and countries. We support healthy and accurate information sharing utilizing existing best practices. We also support the innovation and evolution of

information sharing practices. We welcome an additional direct discussion. Please contact me or Andrew Hoerner at ahoerner@fsisac.com.

Thanks for all your hard work to date, it is much appreciated by industry.

Sincerely

William B. Nelson

President & CEO

FS-ISAC

bnelson@fsisac.com

FS-ISAC Inc.
12020 Sunrise Valley Drive
Ste 200
Reston, VA 20191

Jan 15 2018