Dr. Gregory White
Executive Director
ISAO Standards Organization
University of Texas San Antonio
San Antonio, TX 78249

January 15, 2018

Dear Dr. White:

On behalf of the Information Technology-Information Sharing and Analysis Center (IT-ISAC), and at the request of the IT-ISAC Board of Directors, I am writing in response to the request for comments the Standards Organization (SO) issued on December 1, 2017. Please accept these comments in addition to the input we have previously provided.

Formed in 2000 and achieving operational capabilities in 2001, the IT-ISAC is one of the nation's longest established ISACs. We have been designated by the IT Sector Coordinating Council (IT SCC), and recognized by DHS under the National Infrastructure Protection Plan, as the IT Sector's designated operational entity. We are founding members of the National Council of ISACs and the IT Sector Coordinating Council and have actively engaged in the development of information sharing policy, domestically and internationally, since our founding.

Our membership has grown from a small group of U.S. based security vendors, to a diverse set of global technology companies and companies that leverage IT for critical business operations. Our membership includes security vendors, software companies, hardware companies, home automation and IOT companies, and companies in the food and agriculture community, among others. Key to this growth is focusing on the needs of our members.

We would like to emphasize our commitment to the success of the Standards Organization. The IT-ISAC has supported the work of the Standards Organization and contributed to its success by actively participating in its working groups. In addition, many of our members have contributed to SO Working Groups and participated in various public comment processes.

We remain concerned, however, about the Standard Organization's certification proposal for several reasons. Among these are:

- *The proposal is not community driven:* The community rejected the idea of a certification program the last time the SO initiated a discussion on it only one year ago.

- *The proposal misapplies/misuses the SO's own documents:* SO guidance has emphasized innovation and flexibility and explicitly state that organizations do not need to provide any specific set of services or capabilities to be called an ISAO. However, the SO certification proposal would require verification that an organization provides all the listed foundational capabilities or services to be considered an ISAO.

- *The unintended consequences of the proposal are easy to foresee*: A certification regime increases organizational costs, diverts limited resources to compliance, and creates unnecessary barriers to forming an ISAO, resulting in the formation of fewer ISAOs. It also will hinder information sharing across organizations.

- *The proposal provides unnecessary intervention into the marketplace:* The proposal is designed for a world with hundreds of ISAOs. The ISAO marketplace is still nascent. The SO should give the market time to mature and adjust before it seeks to intervene.

In our comments below, we provide more details on each of these points, answer each question asked in the call for comments, and propose alternative approaches.

**Certification Proposal is Not Community Driven**

The IT-ISAC would like to reiterate our concerns about the Standards Organization decision to promote a certification proposal on its own, without community consultation or support. The initial set of guidance released by the SO was fully supported by the community and reflective of community consensus. In contrast, the Standard Organization's decision to announce a certification program runs contrary to the expressed wishes of the community.

It is important to recall that as the initial set of guidance documents were being finalized, the Standards Organization initiated a discussion as to whether it was necessary or appropriate to develop a certification regime. There was an extensive debate which culminated in an actual vote at a public meeting hosted by the Standards Organization on September 1, 2016. A clear majority of those in attendance voted against a certification program. Regrettably, the SO's proposal now threatens to undermine the foundation of its own documents and has created distrust of the Standards Organization.

**Misapplication of the Standard Organization's Own Documents**

The Standards Organization's certification proposal would require organizations to verify they provide all of the "foundational" services or capabilities identified in Appendix A of ISAO 100-2 Guidelines for Establishing an ISAO to be considered an ISAO. For example, a stated intent of the SO's certification proposal is to affirm an ISAO "performs the five foundational services and capabilities identified in ISAO 100-2 and ISAO 200-1." (line 27 – 28, also see line 44). Since 200-1 is an unfinished draft product, we will focus our comments on 100-2. Unfortunately, the SOs approach represents a fundamental misapplication or misunderstanding of ISAO 100-2 and its Appendix A.

Appendix A of 100-2 lists various services and capabilities that organizations could **voluntarily** choose to implement to meet the unique needs of its constituency. It is a

nonexclusive menu of options. It expressly states that an organization does not have to provide all the identified capabilities or services to be considered an ISAO.

> "ISAO services and capabilities are chosen by the organization and support the needs of its members. ***Of note,* an *ISAO does not need to provide all of the foundational services or capabilities enumerated hereafter to be considered an ISAO***. Rather, the chart included below is intended to provide information about the advantages and disadvantages of each service for evaluation and use by an interested organization on its path to becoming or evolving its ISAO services and capabilities." (page 18, emphasis added).

Other sections of ISAO 100-2 also emphasize that the document provides guidelines and not mandates for organizations to apply as needed to their unique needs. For example, the Executive Summary states "As a set of guidelines and key considerations, this document is not prescriptive in nature." (Page 1). The Introduction states that the document "does not tell an organization the best way to do something or even what specifically to do. . . . This document presents a collection of strategic and operational planning factors for consideration." (Page 1).

This flexible guidance was intentional, designed to make it as easy as possible for communities to establish organizations that meet their needs. The goal was to promote flexibility and creativity and emphasize that ISAOs are free to apply the guidelines practices, procedures, policies, and services that are most appropriate for their organizations. Therefore, the Standard Organization's proposal to require affirmation that an organization provide *all* the listed "foundational" services to be considered an ISAO is clearly inconsistent with the plain text, guidance and goals of the Standard Organization's own documents.

**Easily to Predict Unintended Consequences**

*Makes it More Difficult to form an ISAO*

A key purpose of Executive Order 13691 is to create more ISAOs. This is one reason why the guidelines released by the SO emphasize flexibility and account for the reality that there will be a diversity among information sharing organizations. We are concerned, therefore, that a certification regime will have the unintended effect of making it more difficult for new ISAOs to form.

Certifications create an unnecessary barrier to entry by increasing costs and promoting compliance over flexibility. Further, certifications force organizations to meet arbitrary requirements developed by disengaged third parties rather than the unique needs of their members. Creating an information sharing organization is difficult and costly enough—organizing a constituency, communicating the need, establishing a budget, creating a leadership structure, etc.—without the worry of meeting certification requirements that may not add value to members. Certification would increase organizational cost and require organizations to use scarce resource (time, money and qualified people are always scarce resources) in an extremely suboptimal way with no clear benefit.

*Hinder the Flow of Information*

Certification also places unnecessary barriers to information sharing, at a time when policy makers have been seeking ways to reduce barriers to make information sharing more effective, timely and extended to a larger community. Further, a certification regime poses practical questions related to how certified ISAOs engage with noncertified ISAOs. What happens when a certified organization wants to share information with uncertified organizations? Is the certified ISAO risking its certification, or creating liability issues, by doing this?

For example, consider an established, trusted relationships in which one ISAO is certified but a partner is not. The Certified ISAO (or its members) determines that there is a liability risk in sharing with an organization that is not certified. The result is that entities who could benefit from the information are left vulnerable since they do not have access to it.

It is worth noting that hackers and other adversaries seem to share information very well, and yet, there is no certification body for hacking community information exchanges. That market works very efficiently, is growing rapidly, and their "members" seem very capable - more so every day - despite being "uncertified."

**Market Intervention**

A key argument used by the Standards Organization to justify its proposal is that the community needs to prepare for when there are hundreds of ISAOs. The claim is that a certification program is needed to identify those who are genuine ISAOs from those who just call themselves ISAOs. In the words of the SO's solicitation, one reason for a certification proposal is to help "control . . . who can utilize the ISAC or ISAO title."

It seems odd that after the government intervenes in the information sharing market place with the goal of creating more information sharing organizations, the organization designated by the government to help create more information sharing organizations then seeks to intervene into the market to control the number of information sharing organizations that are formed. The original market intervention creates a perceived problem, so, of course, the solution is more intervention.

While we do not discount the possibility that hundreds of ISAOs will soon be formed, we have not seen evidence in the market that we are approaching this point. At any rate, there is no demonstrated market failure that justifies a certification program. It is highly likely that self-organizing and partner building will take place as organizations enter or adjust to the changing market. Before again intervening into the market based on a guess on how the market might be in the future, the SO should give time for the community to grow and the market to work.

**Questions Contained in the Call for Comments**

The Standards Organization poses several questions in its call for comments. These questions each touch on the issue of trust. The solicitation is framed with a presumption that a certification program satisfactory addresses these questions and is needed to build and maintain trust. It therefore places the burden on the community to convince the SO that there is a better

approach to address these issues than certifications. *However, since the certification regime has already been rejected by the community, the burden should be on the SO to convince the community that a certification program will work and is the best solution.* But the SO itself does not demonstrate how a certification regime satisfactorily addresses the questions. Still, we are happy to respond to the questions listed in the call for comments.

**Question #1: How does an ISAO know what information it may receive from another ISAO or information sharing organization can be trusted to be accurate?**

The SO's certification proposal focuses on services and capabilities identified in ISAO 100-2. While we agree that trust and accuracy are important, these are not among the "foundational" services listed in ISAO 100-2. Further, this question incorrectly equates certification with trust. It is not possible to certify trust. Trust is earned.

Further, it is hard to see how a certification is the answer to this question. Does the SO propose a regime in which an organization is certified to be "90% accurate?" Will the certifying body look at every threat feed an ISAO might subscribe or have access to and score the accuracy of those feeds? Is the SO proposing that a third party have access to sensitive information ISAO members share to determine how "accurate" or "trusted" that information is? Is the SO proposing providing third party certifiers access to sensitive, member-only calls to evaluate the accuracy of individual analysis members share on those calls? These are not tenable options.

Still, there are ways for potential members or partners to glean the type and quality of ISAO information. Organizations can ask to see a sample of information that is shared within the membership. Knowing who the ISAO members are can help companies evaluate the value being provided. A potential member or partner can speak to other members or partners who are already engaged with the potential partner to get a recommendation or evaluation. Hearing from trusted partners and those who are engaged in the organization will carry much more weight with organizations than a certification. Customer referral, not certification, is the best validation.

**Question 2: How does an ISAO know it can trust another ISAO or organization it shares information with will not misuse that information?**

Again, it is not clear what "foundational" service or capability this question addresses. It also is unclear as to how a third-party certification program can guarantee that information will not be misused. In truth, a certification regime would not reduce the risk of information leaking, but it would create barriers to sharing that will reduce the amount of information that is shared.

Trust is earned by experience and by consistently delivering results and value, not through certifications. The Standard Organization's published guidelines provides sound guidance for organizations on how to build trust. The content was provided by organizations that have successfully formed and implemented differing trust models. Rather than building a certification regime that seeks to somehow certify an organization's trustworthiness, the Standard Organization should leverage the trust related content in its published documents and its role as a convener of the community to help build trust within and across the community.

The sad reality is that there is no guarantee that information will not be leaked or misused. However, the solution to this is the market. If information is misused, then the organization that misused the information will have its information flow cut off. Word will get out that the organization cannot be trusted and other organizations will stop sharing with it. This sounds simplistic, but it works.

**Question 3: How can an individual or company wishing to join an information sharing organization trust the claims of the information sharing organization?**

As with any other venture, a potential individual or company can always seek recommendations from current and past members of the ISAO. Members give honest feedback on where an organization adds value and where it does not. This is the way much of any market operates. It is difficult to sell a product or service without a reference. Much in the same way a company will talk with a colleague before deciding the value of joining a local Chamber of Commerce, or before donating to a local charity, getting direct feedback from current or past members will provide much more insight into an organization than a certification.

This model is applied across the economy every day in countless ways. People do not blindly accept a retail store's claim that it sells the best merchandise in the most cost-effective manner. There is no certification program for retail stores, yet through research and customer referral, consumers make informed decisions on what stores have the items they need at the price they are willing to pay.

**Question 4: How does an individual or company know what services or capabilities an ISAO is truly offering and how it compares to those offered by another?**

The essence of this question is to substitute basic due diligence with a certification regime. A company has some responsibility to examine organizations it is considering joining. Many issues can be addressed by companies asking simple questions to the ISAO or to its customers or members. For example, if an ISAO claims that all members have access to a threat intelligence platform, a potential member can ask for a demo of that platform. If an ISAO claims it issues reports, the potential partner can ask for a sample.

This also is another example in which the problem will be addressed by the market. If there is an ISAO that claims that it is delivering capabilities that it is not, it will quickly lose members and partners. If the ISAO has a growing list of trusted companies as members, chances are it is delivering the capabilities and value it advertises.

This question also raises the uncomfortable prospect that a certification regime will be used to "compare" the services and capabilities of one ISAO against the services and capabilities of another. The question implies the certification will not just certify that an ISAO performs all the foundational services and capabilities identified in ISAO 100-2 (which, as we noted, is inconsistent with published SO guidance), but that this process will rate ISAOs against each other. This is highly inappropriate since each ISAO is formed to meet the unique needs of its individual members. Not all ISAOs will require the same level of capabilities or services.

**Question 5: For a company just entering the ecosystem or a new group of organizations that have come together to form an ISAO, how do they know minimally what they should be doing or expecting?**

Such companies should expect that the ISAO meet the needs of its members. If a community is coming together, presumably it is for a specific purpose and/or to address a specific need. The emerging ISAO/community would best serve its members by meeting those needs and achieving its purpose. The ISAO should not be focused on meeting a certification requirement that may not bring value to its organization.

Fortunately, the SO has produced resources that will help ISAOs identify tips, policies, procedures and techniques to help them succeed. We suggest the SO consider creating a guide for companies who are looking to join an ISAO better understand their needs and evaluate what organization might work best for them. This guide could help companies better understand their needs and capabilities to identify how they can best participate in the ISAO community.

**Conclusion**

The certification program outlined by the Standards Organization represents a fundamental misunderstanding and misapplication of the SO's own published work products. ISAO 100-2 clearly provides a potential set of services or capabilities an ISAO could choose to perform to meet the needs of its members. It does not define a suite or set of services an ISAO **must** provide to be considered an ISAO. The plain text of that document demonstrates this to be true. It is very concerning that the SO misapplies the content of its own documents to propose a program that runs contrary to the previously expressed wishes of its engaged constituency.

Further, the proposal runs counter to the Executive Order's goal of creating more ISAOs. By increasing the complexity and costs of creating an ISAO, a certification program will result in the formation of fewer organizations. The opportunity cost of certification is very high, and the community will end up with worse, not better, security. Finally, the SO itself has not demonstrated how its proposed program is an effective solution to the perceived problems.

In contrast, market driven, customer focused solutions can best serve the community. The Standards Organization can further assist the community by:

- Hosting a workshop, or series of workshops, that bring together existing ISACs and ISAOs and emerging ISAOs;
- Creating a new document to help companies evaluate how to choose an ISAO that might be a good fit for their needs;
- Expanding on or highlight the trust guidance provided in the SO's published documentation; and
- Creating a mentor program that pairs emerging ISAOs with established ISAOs.

Collectively, these steps will more quickly achieve the outcomes we both seek in a community driven, consensus based manner that leverages the experiences of successful information sharing organizations to meet the needs of the emerging community. The Standards Organization can play an important role as the facilitator of this engagement as it focuses on

nurturing the development of emerging ISAOs and building trust through voluntary engagement and collaboration. This approach will be both more successful and better received than the development of a certification proposal.

Thank you for your consideration of our comments. As always, if you have any questions or wish to discuss further, please do not hesitate to contact me.

Sincerely,

Scott C. Algeier

Scott C. Algeier
Executive Director