



Mr. Michael Echols
Director, JPMO-ISAO Coordinator
NPPD, Department of Homeland Security
245 Murray Lane, Mail Stop 0615
Arlington VA 20598-0615

July 10, 2015

Dear Mr. Echols:

On behalf of the IT Sector Coordinating Council (IT SCC), I am pleased to provide this response to the call for comments solicited in the Federal Register on May 27, 2015. The IT SCC intends to continue to engage in this process through active participation in ISAO Workshops, as well as through the open comment periods, as they are available.

Question 1. Describe the overarching goal and value proposition of Information Sharing and Analysis Organizations (ISAOs) for your organization.

The IT Sector Coordinating Council believes that an industry driven model, as opposed to a government driven model, is the most effective model for ISAOs. The IT SCC has designated the Information Technology – Information Sharing and Analysis Center (IT-ISAC) as the operating arm of the IT Sector. This has been codified in various iterations of the IT Sector Specific Plan and recognized by the IT Sector Specific Agency. The IT-ISAC and IT SCC work closely and well together, with the IT-ISAC having a designated seat on the IT SCC Executive Committee.

The IT-ISAC provides an effective and efficient method to share operational (as opposed to policy) information amongst the IT Sector and with both government and other partners such as other ISACs. In addition, the IT-ISAC provides an effective forum to pull together subject matter experts from leading companies within the sector to provide collective analysis on threats, incidents and trends.

As new ISAOs are established, they should look to draw on the established practices of existing ISACs. Additionally, we think it also is important that policy makers and those establishing ISAOs should consider the following:

- What organizations are not participating in information sharing and how do we reach them? The goal should not be to get companies who are currently engaging to

participate in more forums, but rather to bring new companies into existing and new information sharing structures, particularly small and medium sized businesses.

- There might be a difference between the type of information that is being produced and the type of information that can be consumed. The capabilities and resources of companies and organizations vary widely. Whereas one company might have the ability to engage in automated information exchange, other companies might not even have an “IT guy.” As such, different organizations may require different information sets.
- More information does not necessarily equate to better information. A key to information sharing and analysis is to prioritize what is important and actionable. Further, if one company shares information through various forums, and those forums then pass along the information to their members, it could create an echo effect in which information that is shared regarding one event appears to be an event experienced by multiple companies.

Question 2. Identify and describe any information protection policies that should be implemented by ISAOs to ensure that they maintain the trust of participating organizations.

Having structured, binding agreements among members is important for maintaining trust, as is a common set of rules applicable to all members. However, while strong legal agreements will be necessary for ISAOs, they will not be sufficient. Trust is critical for the success of information sharing programs. Trust is developed, not certified. There are many ways to develop trust, , including by having an established operational procedure that returns value to members who share information, by vetting members and receiving consistent contributions from them, and by personal and regular engagement among and between members.

Question 3. Describe any capabilities that should be demonstrated by ISAOs, including capabilities related to receiving, analyzing, storing, and sharing information.

It is important to note that an ISAO’s first responsibility is to provide value to its members. ISAOs should be designed and governed by their members to meet the unique individual needs of their membership. The members of the ISAOs themselves must define the role of their particular ISAO and then develop policies and capabilities to meet that role. It would benefit any proposed new ISAO to consider what unique value they add, and how their proposed capabilities might differ from existing structures. That said, there are several common attributes among information sharing organizations. While it should not be required that new ISAOs demonstrate each of these capabilities, they may want to consider whether they should perform one or more of the following roles:

- Information Aggregator: The role of an ISAO in collecting and collating information.
- Information Broadcaster: The role of an ISAO in passing reports from others to their members. This includes the ability to share with or without attribution of the information originator.

- Information Analyzer: The role of an ISAO in collecting raw data /information and refining it into reports.

Question 4. Describe any potential attributes of ISAOs that will constrain their capability to best serve the information sharing requirements of member organizations.

A key reason for the success of many existing information sharing organizations is that they have been driven and led by the private sector. Even where government agencies encourage companies to join their sector specific ISACs, those ISACs are self-governed, self-organized and self-led. This helps establish trust within industry.

Some have raised concerns regarding the degree of actual or perceived government ownership of the current ISAO process. Even the perception that we are moving from a private sector driven model to one that is driven by the U.S. government is bound to be counterproductive, in that may impede the formation of trust amongst industry participants.

Another potential constraint is if ISAOs are not able to provide information to members beyond what is already publicly available. ISAOs will not be successful if they are perceived to share public information or if they just duplicate information that is already being shared. At the same time, establishing a one-size-fits-all approach could constrain the ability of ISAOs to properly meet the unique needs of their own members.

Finally, concerns about the ability to create a national capability from a multitude of ISAOs may act as a constraint. How are ISAOs connected to form a common capability? How are these various individual ISAOs sustained from a dues and membership perspective? What are the incentives to establishing and/or joining an ISAO? Much foundational work needs to be done to define answers to these questions at the earliest stage possible, based on stakeholder input.

Question 5. Identify and comment on proven methods and models that can be emulated to assist in promoting formation of ISAOs and how the ISAO “standards” body called for by E.O. 13691 can leverage such methods and models in developing its guidance.

We have previously expressed our belief that establishing ISAOs should look at the existing models of successful organizations such as ISACs. However, in examining existing successful models, one will quickly note that no two organizations are the same. Instead of having a specific model imposed on them, ISAOs should be afforded the opportunity to develop a model that works best for them by drawing on the practices that work for others when appropriate, or creating a unique capability or practice that suits the particular needs of their members

Therefore, the first priority of the Standards Organization should be to develop flexible standards that can be adapted to many different types of ISAOs. Second, the Standards Organization should look to leverage the practices of existing, effective information sharing structures, without doing harm to those existing structures. Third, the Standards Organization should look at ways government can effectively promote ISAOs or otherwise support their

development, while avoiding the perception that government is controlling these new organizations. Current government practices to promote information sharing are inconsistent in this regard, as some agencies actively encourage companies to join their sector ISAC while other agencies do not.

Finally, in the previous question we touched on the economic model that will sustain the ISAO construct, and we raise it here again. The key to achieving robust operational capabilities is not setting a standard for such capabilities, but the availability of sufficient resources to achieve those capabilities. Establishing and maintaining an operational capability requires financial resources. As a general rule, the more resources available to an organization, the more capabilities they can invest in. The stated expectation is to have several hundred ISAOs established in the next two years. While this may be a laudable goal, it is unclear to us where the resources will come from to develop and sustain these organizations.

Question 6. How can the U.S. government best foster and encourage the organic development of ISAOs, and what should the U.S. government avoid when interacting with or supporting ISAOs?

There are two ways to achieve this. The first is to avoid actual or perceived government control of the ISAO model and ISAOs. Cybersecurity is a global issue and many companies operate around the globe. Actual or perceived U.S. government control over ISAOs or the ISAO model might damage the credibility of the effort amongst international stakeholders, making participation in the effort less appealing to many US-based organizations.

The second is to provide adequate economic incentives to enable the private sector to build and run this model. As discussed previously, this will be an expensive venture, and it is likely that companies will be asked to support multiple ISAOs. What is the incentive and value for them to do so? Will the government be providing seed money to help establish ISAOs or to enable existing organizations to expand their capabilities?

Question 7. Identify potential conflicts with existing laws, authorities that may inhibit organizations from participating in ISAOs and describe potential remedies to these conflicts.

We believe that a significant, under discussed topic is the area of contract I. Companies in the IT Sector possess information about what is happening on our client networks. While this information could be valuable to other companies and help them manage their risks, usually the client as the originator of the information maintains a level of control over its dissemination. This control is often ensured by contracts, often making it difficult for IT companies to share client information with the federal government or other partners. We do not see an easy solution to this issue.

The second issue involves international data protection laws. Many IT companies do business or have facilities overseas, and so are subject to a plethora of international laws related to data

protection and sharing personally identifiable information, complicating our ability to share. It is likely this is not a problem unique to our sector.

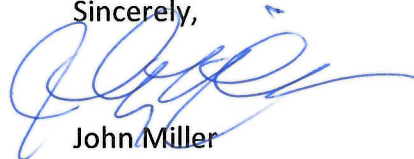
Question 8. Please identify other potential challenges and issues that you believe may affect the development and maturation of effective ISAOs.

In closing, we would like to re-emphasize two points related to this question. First, the extent to which the Government will control, or is perceived to have control, over the development and governance of ISAOs is a big challenge. If the government is seen as controlling who is and who is not an ISAO, and/or imposing a set of standards, then this initiative faces tremendous difficulties. If, however, the effort is industry driven, there is a much better likelihood of industry engaging to self-form ISAOs.

The second point involves the uncertain economics of how ISAOs will be sustained and how these organizations will connect into an overall national capability, rather than merely one-off relationships. Integrating information from hundreds of ISAOs to produce actionable threat information will be a tremendous challenge for the resource constrained NCCIC. Likewise, individual ISAOs likely will not have the resources and capabilities to build and maintain relationships with hundreds of partner organizations. So the question becomes what is the economic model that will sustain this initiative, and what is the operational vision to develop an integrated capability?

On behalf of the members of the IT Sector Coordinating Council, I would like to thank you for your consideration of our comments. Please do not hesitate to contact me if you need additional information, and we look forward to continuing to partner with you as this effort moves forward.

Sincerely,



John Miller

IT SCC Chair