# Internet Security Alliance (ISA) Comments to Department of Homeland Security on the Initiative to Identify Best Practices for Information Sharing and Analysis Organizations (ISAO)

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

April 18th, 2015

The March 4, 2015 Federal Register Notice announcing the March 18th ISAO/ISAC Summit indicated that there was an open comment period through April 19th. The Internet Security Alliance (ISA) appreciates the opportunity to offer our comments as our preliminary input and initial contributions to the ISAO discussion in addition to the statement for the public record ISA made at March 18th open meeting.

For purposes of clarity, ISA does not intend to become an ISAO, and while we are open to and look forward to working with other organizations who may become the prime contractor as the standards organization that will identify the best practices for ISAOs, ISA does not expect to be that primary contractor.

Instead ISA's comments are as an interested and very supportive part of the ISAO process. Indeed, many of the core aspects of the ISAO proposal including branching out of the traditional sector ISAC model and greater access to more actionable information by smaller players, were first advocated by the ISA in our Cyber Security Social Contract (2008) and referenced extensively in President Obama's "Cyber Space Policy Review (2009). ISA anticipates contributing further as the Standards Organization begins its work and at that time will weigh in on the standards themselves.

With respect to the Standards Organization, ISA recommends that DHS consider the following attributes as it begins the process of increasing when selecting an organization:

I. <u>Goal of the Best Practice Process Should be Increased Actionable Information and Improved Overall Cyber security</u>

The ultimate goal of the standards organization in identifying the best practices for ISAOs should not simply be to increase the amount of information shared. The goal needs be an increase in actionable information that increases cyber security. Without an emphasis on increasing actionable information the process to identify the best practices for ISAOs could lead to ineffective and overly bureaucratic organizations that will not generate a measurable increase in overall cyber security. In order to achieve this goal ISA recommends the following objectives be undertaken by any standards body DHS selects to identify ISAO best practices:

1. **Information sharing system needs to be easier to manage with as little government style bureaucracy as possible**
2. **Information shared itself needs to be in a form easy for the recipient to use**
3. **Information sharing system needs to be economically easy to administer**
4. **Information sharing system needs to generate timely information**

II. Need to Get Increased Involvement from SMB Community.

In the cyber threat landscape of today, small businesses and third party vendors are increasingly becoming the launching point for malicious attackers attempting to gain access to sensitive data. For example, the air conditioner vendor who was the point of attack resulting in the Target breach had no commercial incentive to protect Target's data---and expecting Target to become the policemen for the thousands of entities they interconnect with is totally unreasonable and both technically and economically impractical. Through the ISAO best practices process, we will need to find these smaller organizations appropriate market incentives to participate in the system. This has been an elusive goal for decades. Some ISACs, have achieved some success in expanding beyond major players, but for the most part, the inherent barriers of cost, time and insufficient resources, both financial and technical, in small companies has precluded broad based participation.

The truth is every small company wants the same thing---to become a big company. If they have extra resources it is not likely to go to security, it's likely to go to sales and marketing. In developing procedures for the ISAOs this pragmatic fact of life needs to be addressed up front. The assumption that long-term economic risks from cyber attacks will generate active participation by smaller entities has simply not proven to be the case notwithstanding years of publicity about cyber attacks.

To attract smaller players we need to make the system easier for them. Smaller players want info sharing to look like Norton anti-virus. They don't have the economies of scope and scale some larger players can devote to analysis and they don't have personnel they can devote to sit in on daily or weekly technical calls. They just want someone to tell them which button to push to stop attacks. One useful function new ISAOs might undertake, could be to leverage the economies of scope and scale that larger entities have and simplify the information shared to make it more actionable for less sophisticated entities.

III. Standards Organization Should be a Not for Profit Organization and Should Have Experience in a Multi-Stakeholder Process.

A primary goal of the ISAO proposal is to expand active participation of multiple stakeholders in collective cyber security. This is a laudable goal as cyber security is a multi-faceted issue that presents different challenges to different types of entities. As a result the organization that sets rules for the ISAOs needs to be free of cultural bias, though unintended, that may come from a narrow experience with one business type.

The NIPP clearly articulates that government entities understand cyber risks differently than private sector entities do. Even in the private sector, large companies understand cyber

issues differently than smaller ones do, regulated entities understand cyber security very differently than unregulated entities do and entities that operate in multiple jurisdictions have different perspectives than localized entities.

The Standards Organization should also be free of an appearance of a vested corporate interest. It is vitally important that the standards organization be a not for profit organization so that it is not perceived within the community that the organization is focusing on advancing its own commercial interests.

The ideal candidate for setting the rules for the ISAOs should be able to demonstrate not just previous experience with engaging in and/or leading a multi-stakeholder process that results in consensus decision making, but a culture that is inherently multi-sectoral.

## IV. Process being undertaken by Standards Organization Needs to be Industry-Led

To prevent even the appearance of inappropriate government influence in the information sharing or standards development process, the Standards Organization should be an organization that is not a governmental organization or an organization that depends upon a Federal Department or Agency for its operation. As we have already noted, the NIPP clearly articulates that government and industry understand cyber risk differently and hence an organization with strong ties and identity to government or government officials may have difficulty in engendering the trust and support of the broader business community--- especially the outside the beltway community --- that is the major target of the ISAO effort.

Understanding that whatever organization is selected will receive grant funding from the government for this specific project, it is important that the organization is otherwise viewed as independent both technically and culturally from government.

## V. Standards Organization Should Build upon Existing Framework

It is essential that the Standards Organization understands and builds upon the existing information sharing organizations, models, and operations. There is a wealth of experience in how to share information effectively. The Standards Organization should be aware of these efforts and seek to build on the best processes and practices already identified by the current information sharing system – this includes leveraging the work of existing ISACS. To ensure the Standards Organization understands the existing structures, one of the grant requirements might be to meet with and survey existing information sharing organizations to learn about their capabilities and procedures.

While building on the existing model, however the nature of how business is conducted and information managed in the digital world needs to be appreciated and adequate flexibility needs to be built into the system to accommodate these changes.

The multi-sector, as well as international, nature of modern business may not necessarily fit with the historical sector-by-sector model. The selected standards body should examine the most appropriate structures to facilitate information sharing which may be within sectors or across sectors. Effectiveness, not tradition, should be the goal.

VI. Selected Standards Organization Needs to Appreciate the International Nature of Cyber Threat and be Respected Internationally.

Cyber-attacks are international issues, almost always almost inherently. The notion that we can have a US-only solution is as out dated as the notion of perimeter defense against APTs. Since the cyber threat environment is global and information sharing takes place in a global context, the selected standards organization should be one that is recognized and respected internationally. Inevitably, other countries will consider the standards that are developed through this process**.** Therefore it is important that the Standards Organization has a sound reputation outside of the United States

VII. The Guiding Principal for the ISAOs should not be "rules and regs" but Practically Improving the Security of the Cyber System

The reality is that malicious actors have all the advantages. They act faster, they are more nimble, they share information easily and they all have massive economic incentives. If we are going to compete on the same playing field with our adversaries we need to become more inclusive, faster, more action-oriented, and create the proper incentives where they don't naturally exist in the commercial sphere. Understanding there are major trust and legal concerns that need to be considered here, the Standards Organization should consider these in a systematized fashion.

ISA believes that the above attributes will help ensure the community as an independent and impartial organization, with a pristine reputation that is recognized globally, views the Standards Organization and the ability to conduct a consensus based standards development process. This, in turn, will make the resulting standards more credible.

ISA thanks the Department of Homeland Security for the opportunity to comment on this process and we look forward to engaging further as this process unfolds. We would welcome the opportunity to meet with you, if necessary, to discuss our comments in further detail.