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

April 17, 2014

Dear Mr. Echols:

On behalf of the Information Technology – Information Sharing and Analysis Center (IT-ISAC), I am providing this written response to the request for comment noted in the March 4, 2015 Federal Register notice announcing the public ISAO/ISAC Summit on March 18th. We appreciate the opportunity to provide these comments. The IT-ISAC was privileged to have participated in the March 18th meeting and are thankful to have had the opportunity to contribute at that session. For the sake of clarity, we are providing these comments in addition to, not in place of, those provided at the summit.

Founded in 2000 and achieving operational capability in 2001, the Information Technology-Information Sharing and Analysis Center (IT-ISAC) is a non-profit, limited liability corporation formed by members within the Information Technology sector as a unique and specialized forum for managing risks to their corporations and the IT infrastructure. Members participate in national and homeland security efforts to strengthen the IT infrastructure through cyber information sharing and analysis. As a result, members help their companies improve their incident response through trusted collaboration, analysis, coordination, and drive decision-making by policy makers on cybersecurity, incident response, and information sharing issues.

The IT-ISAC Board of Directors welcomes efforts to enhance information sharing within industry and between industry and government. The IT-ISAC has a decade and a half of successful, operational experience facilitating information sharing among members, the federal government and other partners. A key element of this success is our ability to adjust to meet changing member requirements. For example, to meet the evolving threat and the changing needs of our members, we recently implemented a new operational construct which has resulted in a substantially increase in membership and a member retention rate of nearly 100%.

It is important to note that our goal is not simply to share information but rather to develop enhanced situational awareness to enable informed risk management. Information sharing is a tool for achieving this. This is why the IT-ISAC has supported and has actively engaged within the sector partnership model. Under this model, companies are encouraged to join their sector designated information sharing mechanism so that situational awareness can be developed and shared within a sector. This provides important capabilities and efficient communications channels for effective incident response. Most sectors have established ISACs. For those sectors that have not, specific measures should be taken in cooperation with those sectors to establish a formal way to share information with them. To meet the needs of their sector, some sectors, such as transportation have established subsector ISACs. In the rare instance where a company finds that their sectors or subsectors are without an ISAC, or where they have information security needs but are not in a specific critical infrastructure sector, the IT-ISAC has welcomed their membership. For example, companies in the Food and Agriculture Sector are active participants in the IT-ISAC.

The IT-ISAC has worked diligently since its founding to improve coordination among ISACs through the National Council of ISACs, with the Department of Homeland Security (DHS) and other federal agencies. We were part of the 2007 "Tiger Team" that issued a report that recommended the creation of, and provided the framework for establishing, the National Cybersecurity and Communications Integrating Center (NCCIC). We then piloted a program to test a Concept of Operations model developed by the NSTAC Cybersecurity Collaboration Task Force. This pilot successfully demonstrated an effective model for developing national situational awareness through cyber information sharing. We continue to endorse that model and support efforts to improve the NCCIC's ability to serve as a coordinating center across government and industry.

In terms of implementing Executive Order 13691, the IT-ISAC supports the following principles:

- Established sector based, industry led ISACs have the experience and history of successful information sharing and analysis. ISACs should be cornerstones for the ISAO construct.

- Information Sharing standards and best practices should be industry driven, not prescriptive and not overly burdensome.

- The ISAO construct needs to consider the global nature of the threat and information sharing challenges.

- The goal is to achieve situational awareness. Information sharing is a tool that enables situational awareness and informs actions.

When developing the standards, it is important that the Standards Organization engage with the information sharing community to ensure that the standards that are to be developed reflect operational and business realities. The "Gold Standard" should not be the baseline requirement. Instead, consistent with the principles above, the standards must reflect the following:

- **Each Organization is Unique**: Sector specific ISACs, and information sharing organizations more generally, have unique organizational structures. While many ISACs are incorporated as not for profits, the services of other ISACs are provided through direct contracts to third parties to provide these services directly. Some ISACs have paid employees and staff. ISACs have bylaws and member agreements that govern how information shared can be used and how shared, and the roles, rights and responsibilities of members. These policies, procedures and governance structures have all been designed to meet the individual needs of the members, and it is important that these not be disrupted. Standards should enable ISACs and ISAOs to adopt a business model and governance structure that meets the needs of their members.

- **Organizations are Member Driven:** The reason each ISAC is unique is because the members of that ISAC have unique needs. Information Sharing and Analysis Organizations will only be successful if they are enabled to meet the unique demands and needs of its members. As one example, the IT-ISAC is unique since we are asking companies who are competitors in the security market space to share information with each other. Our goal is to provide value to our members, without competing with them. To do this, we have developed an operational model whereby we connect subject matter experts on specific topics with their peers in other IT-ISAC member companies. This enables them to share information on specific threats, identify appropriate mitigation strategies, and conduct joint analysis. This has proven to be a very effective model for us.

- **The Cyber Threat is International**: Many existing ISAOs, including ISACs, are international organizations. Many of our members are global corporations and some members are based outside the United States. In addition, cyber security is a global problem requiring a global reach and whatever standards that are developed here will be considered by other countries. Therefore, the standards that are to be developed should fit within a global context in mind.

- **Information Sharing is a Voluntary Activity:** There has been some discussion that the Standards should consider making information sharing mandatory. This would be a serious mistake. Information sharing mandates would disrupt the voluntary nature of information sharing and will lead to companies providing information that is not of value simply so that they meet a requirement to share. In addition to the regulatory aspect of mandatory sharing, there are very practical considerations such as:
    - What would be the minimum sharing required?
    - How do you measures and compare sharer's contributions?
    - Is sharing quality or quantity-based?
    - Is there a timeliness component of the requirement?

  For these and other reasons, rules concerning information sharing should be developed by the members of an ISAO to meet its particular business model.

- **The Goal is Situational Awareness/Integrated Capability**: Too often people consider information sharing to be the end goal. However, the purpose of information sharing is to create enhanced situational awareness. Information sharing is a tool to achieving this. From our perspective there does not seem to be any strategy to turn individual information sharing initiatives into an integrated, national capability. There is a concern that as more organizations are created, national situational awareness is harder to achieve since there is less sector based analysis and sharing and it becomes harder for both the private sector and government to build and maintain relationships across a larger number of organizations. We urge everyone engaged in this discussion to focus on building a national capability, rather than individual initiatives.

Finally, we would like to note that there remain several unanswered questions surrounding ISAOs and ISACs. Among these are:

- Will the Department of Homeland Security refuse to engage in information sharing agreements with organizations that do not adopt the standards?
- By what basis can an organization certify that it has adopted the standards? Must they certify that they have adopted 100% of the standards, or is there another threshold?
- Are existing sector based ISACs, endorsed by their sector coordinating council under the National Infrastructure Plan process, grandfathered or exempt from the resulting ISAO standards?

To date, the answers to these questions have been inconsistent, unclear, or contradictory. Getting clarity on these questions is important as the process continues.

Thank you for your consideration of our comments. We look forward to engaging in an active, constructive and honest manner throughout this process.

Sincerely,

Scott C. Algeier

Scott C. Algeier
Executive Director