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

April 19, 2015

Dear Mr. Echols:

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 IT Sector Coordinating Council appreciates the opportunity to offer these comments as our preliminary input and initial contributions to the ISAO discussion. We anticipate contributing further as the Standards Organization begins its work, and at that time we plan to weigh in on the standards themselves. We focus this initial input on: (1) the attributes we think are important for the standards organization to possess, and (2) our questions concerning ISAOs.

Regarding the Standards Organization, the IT Sector Coordinating Council understands that this organization will be selected by DHS through the DHS grants process. We recommend that DHS consider the following attributes when selecting the organization:

- **Industry Led**—To prevent 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 survival. While we understand that whatever organization is selected will receive grant funding from the government for this specific project, it is nonetheless important that the organization be viewed as otherwise independent from government. While the receipt of previous federal funding should not preclude an organization from consideration, we believe the selected organization should not be solely or significantly reliant upon government funding.

- **Not for Profit Organization**—In the same way that the organization should be free of the perception of government influence, 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 nonprofit organization to avoid the perception within the community that the organization is focusing on advancing its own commercial interests.

- **Experience with a multi-stakeholder process**—The Standards Organization should be able to demonstrate previous experience with engaging in and/or leading a multi-stakeholder process that results in consensus decision making. The Standards Organization should be able to demonstrate that it can implement an inclusive community of interest development process similar to the one used by NIST in the development of the Cybersecurity Framework.

- **Respected Internationally**—Because 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, the standards that are developed through this process will be considered by other countries. Therefore it is important that the Standards Organization enjoys a sound reputation outside of the United States.

- **Understands the Existing Information Sharing Framework**—It is essential that the Standards Organization understand the existing framework of information sharing organizations, models, and operations. There is a wealth of existing experience regarding how to share information effectively. The Standards Organization should be aware of these efforts and seek to build on them, rather than start from scratch. To ensure the Standards Organization understands the existing structures, one of the grant requirements should be to meet with and survey existing information sharing organizations to learn about their capabilities and procedures.

We believe that the above attributes will help ensure the Standards Organization is viewed by the community as an independent and impartial organization, and possesses both a pristine globally recognized reputation and the ability to conduct a consensus based standards development process. This, in turn, will make the resulting standards more credible.

In terms of next steps and implementation, the IT Sector Coordinating Council urges DHS to provide greater clarification on some key questions related to the ISAO process including the following:

- What happens if an organization that wishes to share information decides not to adopt the standards developed by the Standards Organization? Will the Department

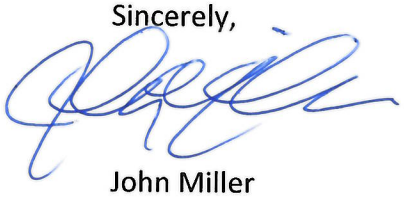
of Homeland Security or other government agencies refuse to share information with that organization?

- What does it mean to "implement" or "adopt" the resulting standards? For example, must an ISAO adopt 100% of the resulting standards to be able to certify that it follows the standards, or is there another threshold?

- Are existing sector-based ISACs that have been endorsed by their sector coordinating council under the National Infrastructure Plan exempt from the resulting ISAO standards? There have been a great deal of conflicting messages regarding whether the ISAO standards would apply to sector-based ISACs whose unique roles and missions have been codified in national strategies such as the National Infrastructure Protection Plan, Sector Specific Plans, and/or recognized by their Sector Coordinating Council or the National Council of ISACs.

On behalf of the IT Sector Coordinating Council, I thank you for your consideration of these comments. We look forward to engaging further as this process unfolds, and would welcome the opportunity to meet with you to discuss our comments in further detail.

Sincerely,



John Miller
IT SCC Chair