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 May 27, 2015 the Department of Homeland Security issued a request for comments on the formation of Information Sharing and Analysis Organizations to support the implementation of Executive Order 13691. Although the Federal Register Notice request for comments identified eight specific questions DHS was seeking answers to, it was noted that responses do not have to be limited to those questions. Consistent with our stated promise to engage constructively with this process, I am providing the below comments, on behalf of the IT-ISAC and with the consent of the IT-ISAC Board, for the Department's consideration.

As this process has unfolded, it has become clear those engaged in these discussion have different concepts of what "standards" mean. Specifically, some view standards as a set of requirements that an organization will implement, while others view "standards" as a set of effective practices that an organization can choose from and apply to their organizations. Considering the diverse needs and composition of existing ISACs and other information sharing organizations, and considering the diverse set of ISAOs that DHS anticipates will be formed as a result of the Executive Order, the IT-ISAC believes that it is most appropriate and useful for the standards to be a set of identified effective practices an organization can pull from to use as needed to meet their unique needs rather than a detailed set of requirements an organization must adhere to. This is consistent with DHS's stated goal of minimizing the impact

to existing, successful organizations while providing a framework for the establishment of new information sharing organizations. This also has the added benefit of following the "first, do no harm" principle that was advanced by several workshop participants in Cambridge in June.

In considering standards development for ISAOs, it is important to emphasize that many of the most effective and long standing information sharing organizations have been successful not because they follow a common set of standards but rather because they respond to the needs of their members. For example, the IT-ISAC was formed in 2000 but we transformed and updated our operational model several times to continue to meet the diverse and ever changing needs of our members.

Organizations must have the flexibility to adjust their business processes, procedures, and practices to meet the evolving needs of their members. In the same way that it would be unlikely that all ISACs would use, for example, the same software, it is equally unrealistic to expect that all their business practices would be the same. Their membership agreements will likewise not have the exact same language and provisions. There is, in fact, no "best practice" in industry – there are a range of good and effective practices. As such, it is unrealistic and counterproductive to standardize business practices.

Similarly, it also is essential that standards align with resources. As with any enterprise, the more resources an organization has, the more capabilities it can achieve. Often the reason why capabilities vary in any enterprise (not just information sharing organizations) is the amount of resources available to them. The reason some organizations are more advanced than others is not that the less advanced lack standards. Instead, they most often lack resources. The economics of where resources will come from to sustain hundreds of ISAOs are not clear.

Time, money and qualified people are limited resources. If a standard dictates you must do specific actions for compliance purposes, then that may crowd out a more valuable use of a scarce resource. Since member needs are diverse and not consistent, organizations should be left to determine how to spend their limited resources in ways that adds value to their organization and members.

The resources issue touches on several additional key points associated with the standards development. First, the most mature capabilities should not be the baseline standard. It is not realistic to expect an organization with modest resources to have the same capabilities as organizations with comparatively more resources. The ISAO guidelines should be flexible enough to allow for ISAOs of all sizes – not all sharing

communities have to be large to be effective to meet their mission, nor do they all have to be capability-heavy. The emphasis should be in supporting right-size communities of sharers with the focus on meeting that community's mission.

Second, in order to have resources to invest in more robust capabilities, an organization will either have to charge high membership dues, thereby potentially pricing out small-and medium-sized companies, or the government will need to help drive membership to these organizations. The government's support of existing information sharing organizations has been inconsistent, with some U.S. federal agencies actively encouraging companies to participate in their sector ISAC while other government agencies refuse to provide such moral support. It is important that there is a consistent, cross government approach to supporting and encouraging companies to join established ISACs and future ISAOs, in addition to ensuring that government provides valuable information for ISACs, ISAOs and their members.

Third, there is more than one way to achieve a capability. An organization should not be evaluated to be more advanced or robust simply because it has more resources or in house capabilities. For example, an organization can have robust analytical capabilities by leveraging the expertise of its members, as opposed to building out a costly internal capability. The ultimate evaluation as to whether an organization provides value should not be through the government or a compliance check list against standards. Instead, the most important evaluation is made by its members.

Fourth, there needs to be further consideration as to how individual ISAOs are integrated into a national capability. For example, established ISACs have developed processes, procedures and capabilities to share across the critical infrastructure community. This includes agreed upon protocols for when and how to share with other ISACs and clarity on how that information is to be handled or further shared. If the ISAOs are to be part of a national capability rather than exist in a series of one-off relationships, then it is important that there is a common understanding of how information can be shared with, used, and disseminated. Further, many companies are global and it may be difficult for them to share exclusively with the U.S. government or U.S. based ISAOs. These companies already have multiple different means of information sharing, so it is important for them to understand how sharing with ISAOs adds value to their current procedures. Otherwise, companies could consider sharing with ISAOs as consuming scarce resources in a very expensive way.

Fifth, while recognizing the need for consistent government engagement with ISACs and ISAOs, the ISACs and ISAOs must continue to be industry led and

industry driven. Even the perception of undue governmental influence in the development of the standards or the organizations themselves runs the risk of driving industry participation away from them. In the same way, due to recent security breaches against several U.S. departments and agencies, there is a concern about the ability of U.S. federal authorities to protect information that is shared with it.

Finally, it is important to consider the need for global information sharing. The ISAOs have to fit with and play well with the international community of defenders. Therefore, the standards should be palatable to the international community. Having them U.S. centric or seen as U.S. centric would be a barrier to information sharing.

The IT-ISAC appreciates the opportunity to provide these comments and we look forward to continued engagement throughout this process. It is our intent to work closely with and share our expertise with the selected Standards Organization. Should you have any questions or if we can be of further assistance, please do not hesitate to contact me.

Sincerely,

Scott C. Algeier

Executive Director, IT-ISAC