Dr. Gregory B. White
Executive Director,
Standards Development Organization
c/o LMI
1777 NE Loop 410, Suite 808
San Antonio, TX 78217-5217

June 16, 2016

Dear Dr. White:

On behalf of the IT-ISAC, the IT Sector Coordinating Council, the Communications ISAC and the Communications Sector Coordinating Council, we respectfully submit the following comments on the documents the Standards Development Organization released for public comment last month.

Before providing our comments, we would like to acknowledge and thank the working group members and chairs who are volunteering their time to develop these documents. Our representatives and members are actively engaged in several of the working groups and have experienced first-hand the commitment and dedication of those involved in this time consuming effort.

We understand that the draft documents are being actively updated and we will continue to engage in this process. We do, however, want to take this opportunity to highlight issues that are important to us and to our members.

Our comments are shaped by several perspectives. First, our sectors have long established and highly capable Information Sharing and Analysis Centers (ISACs). The origins of the Communications Sector partnership with government date back to the 1960's with the creation of the National Communications System (NCS) following the Cuban Missile Crisis and the National Coordinating Center for Communications (NCC or Comms ISAC) was established in 2000. The IT Sector was also among the first sectors to establish an ISAC in 2000. As such, our organizations have vast experience in building, operating and sustaining information sharing capabilities.

Second, our respective ISACs have vastly different business models and operational policies, procedures and plans. This reflects the different needs of the constituent membership of those ISACs. Our ISACs continue to adjust their operational and business models to meet the needs of their members. We believe it is essential that all ISACs and Information Sharing and Analysis Organizations (ISAOs) continue to have the flexibility to meet the diverse needs of their membership.

Third, the primary objective of the Executive Order establishing the Standards Development Organization was to encourage and facilitate the formation of ISAOs to serve communities that are perceived to be excluded from the ISAC model. Specifically, it has been mentioned that the goal is to

make it easier to establish information sharing forums at local or regional levels or for non-critical infrastructure sectors. As such, the final documents released by the Standards Development Organization should constitute high level guidance that organizations can readily interpret and utilize. As with any venture, the more complicated something is, the lower the chance of success.

Fourth, engaging in information sharing is a valuable tool in enterprise risk management, but information sharing alone is not the goal, nor is it sufficient. Instead, information sharing is an important element of a comprehensive cybersecurity strategy. Participating in information sharing forums enables companies to better manage risks, but it will not prevent members from being victims of a cyberattack. It is important that the Standards Organization more clearly state this in the documents to avoid giving false sense of security to organizations who could think that being part of ISAO and sharing/receiving addresses the main security concerns.

With that perspective, we offer the following comments:

- **Guidance not Standards**: It is important to note early in the documents that the Standards Development Organization is not following the formal, internationally recognized method for standards development, and therefore should be considered "guidance" and not "standards." The Standards Development Organization is correctly focusing on developing guidance for organizations about how to approach various issues. The final product should not be considered by the users to be a set of best practices or formal standards, which would imply a thorough vetting process and evidence resulting in a "best practice." What works for one organization might not work for another, and guidance should maintain flexibility that help organizations work through the issue in a way that works for them. Making this distinction clear will help set proper expectations for the document's various audiences.
- **Capabilities:** A key value the final product can provide to ISAOs, and organizations seeking to establish ISAOs, is to identify a suite of potential capabilities or services; however, the Standards Development Organization shouldn't assume a one size fits all model for ISAOs. ISAOs, and organizations forming them, should be free to choose to deploy the services or capabilities that are most appropriate for their membership. In this way, the Standards Development Organization would develop a menu of services that ISAOs could pull from. ISAOs should be free to choose from the menu to meet the specific needs of their membership.
- **Models:** The Standards Development Organization should refrain from developing, promoting, or recommending any specific model of ISAO or models for ISAO business or operations. Since each ISAO is designed to meet the unique needs of their members, there is no one "model" way an ISAO should operate. Even within the existing ISAC community, no two ISACs have the same operating or business model. Proposing, promoting, endorsing or recommending specific models runs the risk of stifling innovation and pushing ISAOs into a structure that is not appropriate for them. Instead, the final document should discuss the various approaches ISAOs may want to consider, identify practices that have worked for others and help provide ISAOs and their members the knowledge and understanding they need to make informed decisions.
- **Resources:** The draft documents contain a lot of thoughtful guidance. However, there is no high-level guidance on how to align these to resources. Organizations, especially those trying to get off the ground, will have limited resources and must decide how to allocate them in a cost effective manner. However, that final product should refrain from telling organizations how

they should spend those resources and should avoid making any specific staffing recommendations. Instead, the final document should serve as a resource that assists organizations in determining for themselves how their resources can be applied in the most cost effective manner to meet the needs of their members.

- **ISAO Maturity:** Across several of the working groups, there has been considerable discussion around the use of the term "Maturity." We caution against, and do not support, efforts to rate or evaluate the Maturity of an ISAO or to create a "Maturity Model" for ISAOs. The one metric ISAOs should be interested in is whether they meet the needs of their members. Whether these needs are met through the sharing of pdf documents via open email or through the automatic exchange of sensitive indicators does not matter. Rating an ISAO's "Maturity" therefore is not a relevant metric. There are potential consequences to a rating system, such as putting a negative light on so called "less mature" ISAOs that are nonetheless meeting the needs of their members, pushing ISAOs into compiling a "maturity checklist" to meet a specific level, rather than focusing on meeting the needs of their members, and creating a maturity level target in the view of regulators and policymakers.
- **Too much discussion on automated exchange:** While we agree that there is value and tremendous potential in automated indicator sharing, we believe the documents focus too much on this topic and that the Standards Development Organization should refrain from endorsing any specific automated sharing framework. This technology remains new and not fully mature. Many large enterprises cannot consume automated indicators, let alone small businesses who in theory gain to benefit the most through the ISAO construct. While a discussion of the value of automated indicator sharing should be mentioned, the discussion should be simplified, and categorized as one potential capability or service in the ISAO menu. A pdf document is of much more value to the average small or Medium Sized business than a STIX file, since that business can open the pdf file but cannot make use of the STIX file. However, it is appropriate and helpful to list in the document, or in an appendix, the DHS requirements for receiving automated indicators through the CISCP and AIS programs.
- **Privacy –**The privacy guidance should focus on encouraging ISAOs to engage with their members on privacy issues and to provide helpful resources for them to institute basic privacy practices that are consistent with CISA and other laws, but should leave the details of those privacy frameworks to member organizations. Putting forward guidance that is too granular or prescriptive runs the risk of discouraging participation in a voluntary process and potentially opening themselves up to liability. Moreover, the privacy guidance should be consistent with existing law and not impose use restrictions or privacy protections that are inconsistent with recently passed legislation. Also, suggesting that ISAOs should take into account European laws and standards may be misplaced here depending upon the information. ISAOs clearly have to follow the respective laws of the countries in which they operate and whose citizen's information is being shared but there shouldn't be a presumption that all ISAOs are sharing information about foreign nationals. We would also be concerned with any document that suggested an ISAO follow international law where it is different from U.S. law. A document that is too prescriptive could also give rise to inconsistencies between the ISACs and the ISAOs rather than promoting complementary entities. Today there is a presumption that the ISACs have been useful, and developing guidance for the ISAOs shouldn't force ISACs to change how they are operating.

- **Certification**: While not specifically addressed in the draft documents that were released, the topic of ISAO certification is one that continues to be discussed within the working groups. The concept of a certification is fundamentally contradictory to the notion of a voluntary risk management framework and will only drive ISAOs to a checklist mentality. However, to the extent the Standards Development Process wishes to pursue a certification process it is our view that certification discussions should be addressed by the standards development community after the final documents are developed. The current certification discussions only detract from this priority. Further, the role of government that was discussed at the Anaheim Workshop on May 18 - 19 was completely inconsistent with the foundational principle of a private sector driven process. Specifically, the notion that government would be a formal arbiter of ISAO to ISAO disputes or ISAO to Member disputes. The ISAO, ISAC and member relationships are bound by voluntary agreements among the parties involved. To the extent that there are disputes or concerns, they should be left to the governance mechanisms developed and agreed to by the parties. In addition, the role of regulators in the standards making process would also be inconsistent with the above principle. Fundamentally ISAOs should be private sector led and managed with minimal government involvement.

We would like to again commend and thank everyone in the Standards Development Organization and working group volunteers for their accomplishments to date and their dedication to this effort. We appreciate your consideration of these comments and intend to remain actively engaged throughout the standards development process.

Sincerely,

Ola Sage
CEO e-Management
Chair, IT Sector Coordinating Council
osage@e-mcinc.com
301.565.2988

Nneka Chiazor
Vice President Public Policy & Government Affairs, Verizon
Chair, Communications Sector Coordinating Council
nneka.chiazor@verizon.com
202.515.2466

Scott C. Algeier
Executive Director, IT-ISAC
salgeier@it-isac.org
703.385.4969

Joseph R. Viens
Chair, Communications ISAC
joe.viens@charter.com
704.731.3841