

January 15, 2018

Gregory B. White, Ph.D.
ISAO SO—Executive Director
Director, Center for Infrastructure Assurance and Security, UTSA

Dear Dr. White:

HITRUST stands ready to support the Information Sharing and Analysis Organization (ISAO) Standards Organization (SO) and the goal of promoting a strong and healthy sharing community. While the discussions at the SO of certifications has certainly raised many concerns within the community, promoting a scalable and sustainable information-sharing environment should continue to be everyone's highest priority.

By way of a small background for context, since 2010 HITRUST has considered itself an ISAO and before ISAOs were given the unique attention by Executive Orders 13691. We were also one of the organizations that fully supported the EO and have been active in the Working Group process from the beginning. We have been a leader at information sharing for some time now, have produced numerous reports detailing the effectiveness of our efforts, and were the first non-governmental organization to join and share bi-directionally with the Department of Homeland Security's Automated Indicator Sharing (AIS) Program. There is not an aspect of information sharing we are not involved with or have not pioneered. As of today, we have over 1500 organizations engaged in information sharing utilizing our CTX platform and representing organizations spanning multiple sectors.

HITRUST began its information sharing program many years ago and it was built on trust and what we call "a loyal fan base." I think if you are a startup ISAO, you must provide participants some level of assurance relating to confidentiality and trust, but we don't necessarily see standards or certification as the only option and certainly something that should not be driven by government, but driven by the private sector. I think we need to find a way to answer the question – "what mechanism is best to give organizations the credibility they need to serve the constituencies they intend to serve." There have been some good suggestions so far and certifications are one of them. ISAOs (and ISACs for that matter) should operate with a minimum set of requirements to instill trust in those they serve. Assurance programs are required to do so, whether self or with a third-party validation and this would benefit emerging organizations. Today there is no mandate to receive certification and it may not be right for everyone but having a process in place seeks to improve the ecosystem for everyone.

During the recent discussion on this topic, numerous ISACs commented that trust was inherited by their participation in the National Council of ISACs. This raises a number of related questions, such as what is the difference between an ISAC and ISAO and should there be a National Council of ISAOs or other entity governing information sharing organizations?

Unfortunately, there is no clarity in the market as to the roles and differentiators between ISACs and ISAOs. The Executive Order recognizes and establishes ISAOs and transitions to that nomenclature as the basis for cyber information sharing, ISAOs have not established a governance structure similar to the National Council of ISACs. As stated by many others, ISACs enjoy credibility by being ISACs where ISAOs do not.

Certification may help this, but there is also a lack of coordination, outreach, education, and interoperability between the ISAOs. While the SO may speak for ISAOs in general, perhaps the discussion going forward should include a discussion on defining the differences between ISACs and ISAOs, if in fact they are different, documenting those differences, defining the role of ISAOs and weighing the merits of having a sister organization to the National Council of ISACs. Serving as a non-governmental voluntary organization that represents ISAOs and helps coordinate any accreditation or standards for the marketplace to provide that same level of trust afford to those that participate in the National Council of ISACs and to support coordination, outreach, education, and interoperability with the ISAOs. ISAOs continue to struggle to have a champion in the marketplace to help address the growing needs they may require.

We all agree that credibility and trust are earned. The SO has been mandated to set them up for success. Certifications are only one mechanism.

Sincerely,

s/ *Carl A. Anderson*

Carl A. Anderson
Chief Legal Officer and Senior Vice President for Government Affairs