CRI
CYBER RESILIENCE INSTITUTE

ISAO Certification Model – Comments to the ISAO Standards Organization

December 28, 2017

The Cyber Resilience Institute (CRI) is a nonprofit organization that promotes cyber resilience building at the community level through activities like information sharing. CRI is engaged in constructing models for these efforts, including use of ISAOs, and embraces the vision in the Executive Order 13691 that ISAOs that engage in public-private exchange of cyber threat intelligence play an important part in improving the cybersecurity posture of the nation. We offer these comments, which broadly support the proposal to establish a certification regime for ISAOs, to encourage further efforts to mature the commercial efforts underway to improve the cyber resilience ecosystem.

CRI believes that the conversation around establishing a certification regime for ISAOs should be broadened. The proposed model, a two-piece construct of self-certified and third party certified tiers, is suitable as a start, but the five foundational ISAO capabilities are insufficient to meet the intended goal of promoting trust. Moreover, the goal itself is too narrow. Trust is a highly essential facet of the information sharing ecosystem; however, the broader strategy of advancement of an industry that improves the nation's security through information sharing necessitates a broadening of objectives after better defining the problem at hand.

The ISAO SO purports, through this and other initiatives, to "elevate the security of our nation". And, it sees in this objective a call from Executive Order 13691 that the private sector should participate in this mission alongside government, particularly in collective information sharing activities and the formation of ISAOs. Consistent with this scope, CRI proposes certain seminal and defining questions to help shape questions about the role of ISAOs in this national effort:

1. With the vision of the stand-up of hundreds or thousands of ISAOs engaged in the production of cyber threat intelligence, is it desirable to maintain and to promote a free flow of cyber threat information across ISAOs?
    a. What are the incentives to share cyber threat intelligence on a free-flowing basis?
    b. What are the consequences of the certification regime on the desired flow?
2. Is there a market for cyber threat intelligence, and is monetization of cyber threat intelligence a likely outcome the advancement of ISAOs?
    a. Is monetization of cyber threat intelligence a positive or negative for advancing the goal of elevating the security of our nation through broad-based information sharing?
3. Is there a social benefit intended in the establishment of hundreds or thousands of ISAOs, and if so how is that factored into the certification regime?
4. Are market forces a desirable influence in the stand-up and build-out of the ISAO ecosystem – is it an industry?
5. Can market forces be married with a national security mission in the ISAO ecosystem or industry? If so, how?

These questions, and we surmise there are many more, pivot around the central question about how industry and government can collaborate in a shared mission space of cyber threat situational awareness and creating a shared repository of cyber threat intelligence that operates to improve the nation's cyber resilience posture. This is, in our judgment, the raison d'etre for the establishment and promotion of ISAOs. Accordingly, a mechanical and narrow approach to ISAO certification would represent a missed opportunity to better shape the emergence of the ecosystem, and risks sending us down the wrong path before we have properly scoped and defined the national objective.

These comments are provided by the undersigned, on behalf of the Cyber Resilience Institute. Please contact me with any questions.

Douglas M. DePeppe
Board President, CRI
Co-Founder, Sports-ISAO
Colorado Springs, CO 80919