From: Scott C. Algeier [mailto:salgeier@it-isac.org]
Sent: Thursday, November 9, 2017 11:49 AM
To: 'Greg B. White' <Greg.White@utsa.edu>; 'Cybersecurity Policy Solutions LLC' <markb@cybersecuritypolicy.com>; 'McGrath, Betsi' <emcgrath@mitre.org>; 'Norma Krayem - Holland and Knight' <norma.krayem@hklaw.com>; 'Douglas DePeppe' <doug@eosedgelegal.com>; 'Nick Sturgeon' <nick.sturgeon@pondurance.com>; 'Deborah Kobza (GICSR' <deborah.kobza@gicsr.org>; 'Landfield, Kent' <kent_landfield@mcafee.com>; 'Frank Grimmelmann - Arizona Cyber Threat Response Alliance (ACTRA' <fgrimmelmann@actraaz.org>; 'Jill Fraser' <jfraser@jeffco.us>; 'Roger Callahan - Information Assurance Advisory / FSISAC' <roger.callahan@iaadvisory.com>; 'Turetsky, David S' <dturetsky@albany.edu>; dbsula@gmail.com; 'Denise Anderson' <danderson@nhisac.org>; 'Richard Barger' <rbarger@splunk.com>; carl.anderson@hitrustalliance.net; 'Fred Hintermister' <Fred.Hintermister@eisac.com>; 'Joe Viens' <Joe.Viens@charter.com>
Cc: 'Lipsey, Richard' <rlipsey@lmi.org>; 'Shreffler, Allen D.' <ashreffler@lmi.org>; 'Natalie Sjelin' <natalie.sjelin@utsa.edu>; 'Larry Sjelin' <Larry.Sjelin@utsa.edu>; 'Cook, Marlis C.' <mcook@lmi.org>; 'DENNIE, Debra' <ddennie@lmi.org>; 'Shabat, Matthew' <matthew.shabat@hq.dhs.gov>
Subject: RE: Message to Working Group Chairs

Hello Dr. White:

Thank you very much for the email and for the additional details around the SO's thinking in regards to developing a certification process. I apologies for my delayed input, but I had travel to Tokyo this week.

As you know, when this topic was last discussed, the IT-ISAC opposed the creation of a certification regime. Since the announcement on this topic last week, I have discussed this issue with the IT-ISAC Board. The IT-ISAC remains opposed to this proposal both on process and policy grounds. We also have a proposed path forward, introduced at the end of the email, which we hope will be considered.

First on process.

- This topic was discussed early and often throughout the development of the initial guidance documents. When the topic was tabled last year, it was because a large majority of the community was opposed to developing a certification program. As a participant in those discussions and an attendee at the meeting when this was tabled, I would like to note that it was not tabled with the provision that the SO would release its own proposal after a year. Instead, the topic was tabled for further discussion within the community after the guidelines had time to germinate and be used. The expectation was that the community would re-engage on the discussion at a later point, not that the SO would decide this point on its own.

- Announcing a certification program ahead of consultations with the community has skewed the debate and placed unnecessary pressure on the community to achieve the pre-announced outcome favored by the SO. Although the below SO statement does include a quote from Mr. Lipsey that the SO is open to other ideas, the SO position seems to be that a certification program is needed and the burden is on the community to talk the SO out of this path. This is the exact opposite way a community driven process should work. The community decided to not pursue a certification program. If the SO has a different position from the community on this, that's fine. But the SO should convince the community of its position before it announces a policy that the community previously rejected. Any announcement on this important topic should reflect the decision of the community, not the position of the SO. This is one reason why the comments about potential opposition from the ISACs (or any other member of the community who opposes a certification program) are so disappointing. While I appreciate the clarification in your note, the fact remains that the SO is the one taking a public position that is contrary to what the community decided when we last discussed this topic.

- One important issue that has not, to our knowledge, been addressed is that there are representatives within the SO advisory leadership team from organizations that have the potential to benefit financially from the development and implementation of a certification program. This issue has been raised in the past and it remains unclear what, if anything, the SO is doing to eliminate this conflict of interest.

On policy, I will summarize some of the many reasons why we oppose certifications (in no particular order).

- Creating a certification program goes beyond the scope of the Executive Order that established the SO. If the EO calls for the development of a certification program, I have not been able to find that section of the EO.

- Certifications will not address many (indeed most) of the issues outlined in the statement and email below. In the interest of brevity, I will not address them all individually, but a certification does not tell me what information an ISAO has, who its members are, or how it will add value to members or partners. A certification does not create trust and it does not give potential members or partners the information they need to determine whether there is value in joining or partnering with that organization.

- A certification program will inevitably move organizations from a mission based approach to a compliance based approach. The community has long discussed and agreed how it is important for ISAOs to meet the unique needs of their individual members. This will naturally result in the creation of all sorts of ISAOs with different missions, scopes and models. This diversity, in fact, has been stated to be one of the main goals behind the EO. Introducing a certification regime will limit this creativity and could discourage the creation of ISAOs and/or make them more difficult to form. In short, a certification regime will move organizations from a focus on member needs to a focus on certification compliance.

- It has been stated previously and implied below that one reason a certification program is needed is to help DHS understand who they should work with. This introduces the very clear possibility of regulation and compliance. If DHS says it will only share with ISAOs that are certified, then this is, in effect, regulation and not a voluntary program. It would require a certification in order to receive information from the government. Organizations with established trust relationships with DHS will now need to be certified. In order to get information from DHS, new ISAOs will be required to go through the time and expense to certify (or to be certified by a third party). Further, ISOAs that might be sector based likely will face interest from their sector's regulators. Companies likely will soon face requirements through regulators and procurement policies that they can only participate in certified ISAOs. The unintended consequences of this are real and have not been fully discussed. As one such example, while everyone was told that use of the NIST Cybersecurity Framework would be voluntary, regulators throughout the world are now looking at ways to regulate the use/implementation of the NIST Cybersecurity Framework.

Instead of focusing on the development of a certification process, we submit that it would be much more beneficial to discuss ways to build trust within the community. Building trust among ISAOs and learning more about them will do much more to facilitate collaboration than would a certification program. One simple but potentially effective way to do this could be to convene a meeting among established ISACs and ISAOs with new/emerging ISAOs so that they can know who they are, what they focus on and can get to know each other. Getting this initial engagement across the community could help foment individual relationships that will help build trust across organizations. This event would be much smaller in scope and scale than the conference that was just held. Attendees could be limited to established ISACs and those ISAOs that have registered with the SO. If there is interest in such an event, I would be happy to participant in the event planning team.

Thank you very much for your consideration.

Scott C. Algeier

Executive Director, IT-ISAC

+1 703-385-4969

salgeier@it-isac.org

IT ISAC