From: John DiMaria [mailto:John.DiMaria@bsigroup.com]
Sent: Sunday, December 10, 2017 10:32
To: Lipsey, Richard <rlipsey@lmi.org>
Subject: [EXTERNAL] BSI Response to the ISAO Request for Comment on certification of information sharing organization (ISACs)

Richard, Hello

Your name was passed on to me as a contact I submit comments to regarding the ISAO activities and the proposed certification process in regards to information sharing associations.

First just a word about BSI:
Global network: 80,000 clients in 172 countries. 67 Offices world-wide
Experienced: The world's first National Standards Body established in 1901

BSI is the oldest National standards body in the world and co-founder of ISO (International Standards Organization). The BSI Royal Charter describes our commitment to improve businesses and the communities around the world by improving performance reducing costs and being an enabler of sustainable growth. Every dollar that BSI takes in is invested right back into the company

We are the leading body of knowledge, creating hundreds of standards a year, many that go on to be ISO standards such as 9001, 27001, 14001. We are the world leader among certification bodies and information security having issued 45% of all the 27001 certifications and 65% of all certifications in the US.

First, for the most part information sharing associations; while they have a formal name, are not legal entities with a formal organizational (corporate) structure. Therefore we do not believe that a formal 3rd party certification process would apply or be applicable in this case, as that would require a formal "Management System" and many of these people have day jobs. If there are formal legal entities 3rd party certifications may apply, but there would still be a large part of those organizations managed by external parties (not full-time).

We agree with previous comments submitted that certification does not technically equal security. You can't inspect in security. There are personal responsibilities of the organization which is why we measure "effectiveness", raise non-conformities and those NCs must be addressed deploying root cause analysis and corrective action that is then verified and effectiveness confirmed . That is where the value comes in……continual improvement, not just a checklist system.

Reading your proposal we also question the ISAO SO's authority to develop a certification process in the first place. Based on Obama executive order which led to the establishment of the standards-writing group and the content which you put forth, it is obvious that that the ISAO has very limited; if any competence in this area at best.

The ISAO is not a member of the IAF (International Accreditation Forum) and it also manages the information sharing program used by the ISACs and therefore has an interest in the program, therefore the ISAO acting as an accreditation body would be a huge conflict of interest.

First to be clear, there is no such thing as “self-certification” only self-declaration. You cannot audit your own work and declare you are certified. Further if it is allowed for anyone in the information sharing community to create several different certifications, you run the risk of the “cowboy” mentality of no formal oversight and a watered down system with no consistency and then you WILL create significant barriers to entry for newly forming ISAOs, and jeopardize the viability of currently functioning, healthy ISAOs.

What you have described in your “self-certification” process has no substance what so ever and is totally meaningless. “without reference to specific means, methods, or technologies that an ISAO employs” How do you know how information is handled, processed and protected?

You say all of this and then say “It is acknowledged that self-certification will not by itself engender a great deal of trust” What’s the point?

A good meaningful “self-declaration” process is a control based questioner grounded by an accepted international standard that is filled in and denotes whether or not the control is applicable or not (with justification), if applicable, and they are in compliance they can summarize in an evidential statement how they are in compliance referencing internal or external documents, policies etc. If not in compliance they can document what actions are being taken to address the issue. At least this will be auditable in the event of a breach or indication of non-compliance and there could be a right to audit. Those self-declaration questioners can then be posted on the website for anyone to read. This is a standard proven method used by many industry standards groups. It shows a level of transparency and does uplift the level of trust because it has substance and tied to an accepted “standard of care”.

If you have been involved with the NIST workshops over the past few years, you may recall that (based on an inquiry from NIST) BSI developed and presented a third party certification model to the NIST CSF. See attached stories released. Due to the interest and positive feedback, we subsequently issued an RFI on the process, presented again at the 2017 workshop and then moved into pilot mode.

We feel it is necessary that we have a deeper discussion between BSI and the ISAO since BSI has already developed a framework for 3rd party certification, just finished a successful pilot just this week and now have a hardened process that is scheduled to be launched in Q1 2018.

3rd party certified has to show that an organization has a robust information security management system in place tied to an international standard. The CSF is very clear that it is not meant to be used in isolation.

We believe our process is already ahead of this idea and as the largest standards body in the world and co-founders of ISO, our standards and certification processes are known throughout the world.

Having said all of this and based on the poor quality and lack of substance contained in the ISAOs proposal, we believe you need to step back and perform more due diligence and obtain a better understanding of what is involved in putting together a robust meaningful value add process and what that might look like.