Information Sharing and Analysis Organization (ISAO) Standards Organization (SO) 3rd Public Meeting

Public Comment And Debate: Standards Working Group 2

Speaker: Joe Vines, SWG2 Core Development Team

Joe Vines, SWG2: So, Brad Howard has been our support guy from the Standards Organization and we are going to put that into further practice during this review because I don't profess to be the expert in the capabilities work group I'm just going to convey some messages on behalf of Denise, Fred, and I think Brad will help to fill in some of the gaps that I may not be able to address with this group.

Having said that, the first thing that occurred with the capabilities group is we developed some core principles around how we would be guided through this process and developing this guidance that we have been asked to do. One of the core principles is that this is voluntary. It's not a mandatory process. It's optional. The other one [core principle] is really based on member driven needs. What the member's need, should really dictate what the ISAO should be. It shouldn't be an arbitrary predefined, prescriptive set of rules, one size fits all; it should be member driven. Easily adaptable so any organization or group can take the document and use it to implement or develop an ISAO. As Frank mentioned earlier, be descriptive, I don't know if he said descriptive, but he said not to be prescriptive so our mantra is be descriptive and not prescriptive. So create a list of capabilities or we are actually going to make a proposal to change the name of this working group from "Capabilities" to "Service and Offerings" because we think that better defines or describes what we are trying to do here. Having the descriptive and not the prescriptive model, a perspective ISAO can cherry pick items based on what their members needs are. Create a list of things that they ought to consider while they are working to stand up their ISAO. A couple of things in our preliminary document that has been posted out on the website, we are calling it 1.0. We categorized areas that are classifications that prospective ISAOs can look at. So, you know, one might be foundational and another might be additional and the other one is unique. The foundational would be just a standard method to send and receive information, kind of a basic capability or service offering. The other one would be additional, enhanced capability beyond those of the foundational, specifically looking at analysis which can help assess and maintain relevance of the membership needs. Unique would be kind of the third one. Common lexicon, understood by all members, research and event programming development, active defense, resilient stock, so on and so forth. I'm not going to go into all of it. I'm sure all of you have read our draft document. That's kind of the gist of what we are doing. Again, basic voluntary capability, collection of foundational items, subset aspirational and optional, which is going to accelerate inter-ISAO collaboration. Our tactics, obviously we are going to negotiate through the work group, the (FAU) Foundational, Additional, and Unique concepts and then we will further discuss elements on the basic voluntary elements for inclusion as well. That kind of leads me to the next phase of this for 2.0. Yesterday, we spent a fair amount of time. There was just a few of us, but I think we were productive in our efforts to drill down further into some of the concepts that we developed in

1.0., and some of the categories that we are going to be addressing in this process are ISAO info sharing and analysis platform. So, under the collect and disseminate data, allow forum to collaborate, ability to analyze. That's some of the items; I'm not going to read all of the items but we will have that out there. We have sent it out to the core members.

The next one will be Member. We will focus on and drill down on the member, member fostering, member collaboration, ISAO cyber work force development, member vetting, regular member meetings, broadcast alerts, things like that, conferences, workshops, webinars. We are pulling a lot of this from existing practices that the ISACs have, as well, that have been pretty successful.

Another category is threat and vulnerability management, CVE publications after polling, adversary TTPs library, and ability to share timely and actual information. Special interest groups provide member support to unique communities of interest. Denise Anderson mentioned a subgroup on medical devices within the healthcare ISAC which meets on a regular basis. In the comms [Communications] area, we have a network service provider group that meets on a weekly basis, every Monday morning at 10 a.m. So, delving deeper into those examples might be beneficial to perspective ISAOs as well and carry those practices forward, if it meets their members' needs. Operations, ISAO community response plan, that can be an item, exercise planning participation, emergency notification system capability, the ability for an ISAO to reach its members during an incident, things like that. Mutually aid others when needed. That's some of the things from a tactical perspective are already occurring in ISACs as it relates to specific incidents like hurricanes and things like that I can speak to from a communication perspective. It's very integral part of our ISAC is the ability to work with one another and be of support to one another during a critical time.

And then finally, the last category is cyber security program management, identity and access management, a reach back service offering, got to get rid of the capability word. To maybe provide a subject matter expert to members if there is a specific issue that somebody is encountering; to have that capability to share service offering within the ISAO to be able to call upon a subject matter expert to help them. Ability to handle non-attributable information as well, not everybody that is involved in an ISAC or ISAO necessarily wants to have attribution. Matter of fact, providing the ability to not attribute statements from somebody actually promotes, in a lot of ways, information sharing. Those are some of the things we are going to be working on in 2.0. I think Brad had a couple of comments as well and then we will go on to questions.

Brad Howard, ISAO SO: I wanted to also touch on what Rick and Frank spoke about a few minutes ago. The overlap we are going to have, and that we do have, in the newly named services and offerings with this particular working group touches on just about every other working group. If you are doing information sharing or doing security and privacy functions, capabilities will definitely touch in that area as well. We are going to be working, as we did yesterday with the other leaders and also involving the core development team members, in making sure that all of those touch points are addressed and we can maximize efficiencies. Well, I think at this point we will turn it over to questions and comments and other inquiries.

Q/A

Q. **Mike Echols, DHS:** in your document you talk about those basic capabilities and services then additional services, so I know we don't like the word maturity, but as an ISAO starts, and they progress through a maturation process, is there going to be anything on the front end to help them understand what the next step is from where they start?

A. **Joel Vines, SWG2:** That's a great question. If you go back to our categories, foundational, additional, and unique, all of that will be and is already initially spelled out. Correct me if I'm wrong Brad, I believe without calling it a maturity model or process, there will be information contained under these three categories; Foundational, Additional, and Unique.

A: **Brad Howard**: There will be some list of what you would normally find in foundational, but again, every service and offering that is going to be out there is going to be member driven. In one particular ISAO, you may have certain services or offerings that an ISAO wants to have that would normally be found in a foundational but also may be found in additional just to meet the needs of the members. Some members may have a more evolved sense of how to do the information sharing and analysis and therefore, their initial set of services and offerings would be a little different from someone who is perhaps not as sophisticated and wants a more simplistic capability to receive information and be able to act upon it. AIS is one that may be for some ISAOs or members the way they wish to have their information transferred to them. Others simply want an email fax or a text alert message that comes through. While we did identify Foundational, Additional, and Unique, it's really going to be member driven on what is going to be cherry picked or selected as a service or offering by each and every ISAO so it's going to be requirement driven in order to support their cliental.

Q. **Roger Callahan, FS ISAC:** I had two questions when reading through this section. There was a lot of discussion about a basic voluntary capability. There was some discussion about a symbol associated with that. Is there some kind of *informata* or what's that driving at?

A. **Brad Howard, ISAO SO:** Fred Hintemeister had taken a look at what they call the basic voluntary capability, the BVC with an icon and that's really in a state right now where it's… I would really prefer to have Fred address that and I'll make sure he gets a comment back posted on the website to address the icon-ization of that particular capability. Sorry I can't answer it fully.

Q. **Roger Callahan, FS ISAC, Cont.:** Second question was, there's a section on compatibility with measures of effectiveness. Continue with some improvement, can you give a little bit more with what the thoughts are there?

A. **Brad Howard, ISAO SO:** Yes, the measures of effectiveness is going to be an internal review by an ISAO recommended that they take a look and see are the services and offerings they have, do they have an effective behavior and reaction to their membership and is there a way to improve it to move on to add further methods to improve effectiveness and efficacy towards their membership.

Q. **Frank Grimmelmann, ACTRA:** You listed a phenomenal list of capabilities that my commendation to your team for being so comprehensive and addressing it. The one I did not hear, I may have just missed it because it was a comprehensive list, was training and education. Is that part of the capabilities you're evaluating at this point?

A. **Joe Vines, SWG2:** That would be under probably operations or member driven. Again this is fresh, hot off the press. We are further developing but I know that it is in there and we discuss that pretty lengthy,

A. **Brad Howard, ISAO SO:** Some of them that were conferences, workshops, it was webinars, newsletters. I know that FS ISAC puts out a monthly newsletter which is very informative but yes, we had workforce development within the ISAO itself and also other educational means and methods for the membership themselves.

Joe Veins, SWG2: Please, we are looking for comments so if you could certainly take a look at the document out on the website and provide the feedback we would very much appreciate that.

ISAO SO Note: This transcript contains edits from the original recording for presentation in written format.