

**Information Sharing and Analysis Organization (ISAO)
Standards Organization (SO) Public Meeting
LMI Headquarters**

7940 Jones Branch Drive, Tysons, VA 22102

November 9th 2015, 7:30 a.m. – 5:00 p.m.

Audience Q&A

HEIDI GRAHAM: Thank you. I'd like to reiterate what all of the moderators said: that we asked you to gather information in many different forms; to provide us information in many different ways today; and we appreciate you doing that in all of the different ways that you worked today.

We're going to give you an opportunity now for some open discussion time. First off, I want to acknowledge that the time that we're going to give you is probably not enough for everybody to have an opportunity to say what they want to say. We're going to have a more open discussion time in future meetings but we thought it was really, really important to gather as much information from you as possible and give you a chance to get to know each other in a more structured way. Before I start the open discussion I'd like to ask for consideration of two ground rules. One of them is: when you're up at the mic please limit your comments to a minute so that we can provide everybody an opportunity. It's not my nature to, but I will jump in at the minute in mid-sentence wherever you are and let you know that the minute is up. Also, I'd ask, if at all possible, as you're providing your comments and your input, please phrase them in terms of a recommendation or a solution so that the folks in the ISAO SO can take on those recommendations and those solutions and get better.

That said, if you have a question, Rick, Bryan, and Dr. White will be available to answer questions if you have them. So, the mics are to the far corners in the middle of the room on the right and the left. If you would like to go ahead and speak, please feel free to go ahead and approach one of the mics. I'll check first if we have anybody in the South conference rooms. Okay, so I think we have everybody here and we'll just go ahead and alternate from one mic to the other. Would anybody have anything they would like to share with the large group?

JIM MCCABE: Hi, Jim McCabe of the American National Standards Institute. It's more of a question than a comment, really, about the timeline because I've heard, you know, you got all this data from here today. You're going to go back and analyze everything that was from the prior workshops, and you've got an aggressive timetable to get something out in terms of preliminary deliverables end of February and then there's also a call for additional data, I think. Is there anything more you can talk about in terms of what those deliverables might be and more specifics around the timing of when things are going to happen? (Just because the holidays and stuff are coming up.)

GREG WHITE: I'll go ahead and see if I can take a shot at that. Deliverables: yeah, a bunch of stuff. We hope, as it was mentioned before, primarily—the major thing obviously standards, but templates, guidelines, processes and procedures, all those kinds of things. Now that said, we harbor no illusions about how long it's going to take to develop certain standards. We know that there are going to be—you saw like you said that aggressive timeline. We fully recognize that there are going to be certain topics—certain standards that are going to be developed that are going to be more complex; that will take more time; that will not be completed by not only February, but it might not be completed in that first year because the discussion will need to continue. At the same time, we think that there are some

other things, especially some best practices, some guidelines, maybe some templates that can be used (as Natalie mentioned) for organizations and entities that are trying to form those ISAOs right now that we can get out soon. So those are the things that we anticipate getting out in the February time frame. I don't anticipate seeing a lot of standards being mentioned in February. You're going to see some of those—if you will—easier ones that will come out shortly after that in that time frame that you saw. But the one thing we don't want to wait on is to get everything together—one big package—and then say, “Here it is! Here is the entire set of standards, the templates, the guidelines. Boom! Publish them at the same time”, because people can't wait. There are, like I said, entities forming ISAOs right now and we want to help them so that they may not go off on a tangent somewhere that they're going to have to come back from later. I don't know if that answers the question.

HEIDI GRAHAM: Alright, who would like to go next?

ERIC BURGER: I'll follow up on Jim's question because I'm not quite sure, I guess. So what I'm hearing is that for February, we're basically going to say, “Hey, we talked to a bunch of people and this is what they're saying.” We're not doing any standards, right? We're not doing—because when you say a template or, you know, processes and stuff, that sounds like a standard which I would think you'd probably want community review. Or is there no plans for community review for that? That, you know, you kind of just churn out right when you get—when you think you've got something you can give people.

HEIDI GRAHAM: Sir, if you wouldn't mind stating your name and organization.

ERIC BURGER: Sorry.

HEIDI GRAHAM: Thank you.

ERIC BURGER: Eric Burger. Georgetown University.

HEIDI GRAHAM: Thank you.

GREG WHITE: Okay, let me—let me—obviously I didn't do a very good job of answering it. What we're talking about for February is: we're going to go through—cull through all the information that we received today, the data call that is going to be coming up. If you remember that rough timeline that was shown in the early part of the day, by February we're going to try to have—we're not going to try-- we're going to go ahead and stand up a number of the different working groups. We're going to identify those working groups and have them stood up and have them starting to meet. Well, there's no way they're going to be able to have a standard created in one or two meetings that they might be able to have before the February second open forum. So, we don't anticipate a lot of standards. We don't anticipate any of the standards. What we think we may be able to find or identify are probably more best practices, probably guidelines on how, “Okay, so you want to start up an ISAO. Where do you start? What's step one?” Those kind of documents. Those kind of guides to help an organization or a group of entities that want to form an ISAO. Those are the kind of things that we anticipate having by the February time frame.

HEIDI GRAHAM: Alright. Who'd like to go next? I'm going to take the microphone to my left if that's alright, sir, and then we'll follow up with you. Thank you.

SCOTT ALGEIER: So, thank you. Good afternoon. Can you hear me?

HEIDI GRAHAM: Yep.

SCOTT ALGEIER: Great. Scott Algeier with the Information Technology ISAC. I appreciate the clarification about the timeline because I had—I was the one who had those questions earlier in the morning, so that's great. Thank you. Regarding the working groups, what's the next step in identifying—how do we identify what the next working groups are and who's on them? When they meet? Whether we're focusing on the right areas in those working groups? What's the next steps in establishing and creating the missions for those working groups?

RICK LIPSEY: Thanks very much for the question, Scott. The intent is, coming out of this initial public meeting today, we are going to combine the analysis and synthesis of information from the previous workshops (that I alluded to earlier this morning) with what we received today. So, the session that you were in with Brad Howard was really focused on the "What". We're going to take a look at that "What" and put that together with the inputs that we get from the earlier meetings into some logical buckets that make sense: "Okay, this is a logical basis for a working group"—informed by the discussions held in Daniel's room that were talking about the process and the nature of the working groups. That's how we're going to package that. So I can't tell you what that is today, but that's what we're going to be working on for the next several weeks. Then we'll go—we'll initiate the process of a call for nominations for leadership positions on those working groups to get them formed and running.

SCOTT ALGEIER: Thanks.

RICK LIPSEY: You bet.

HEIDI GRAHAM: So thank you. As I pass the mic to my right I'd ask the speakers to go ahead and state their name and organization clearly and speak clearly into the mic so that we can get a great recording of this session. Thank you.

ROGER CALLAHAN: Roger Callahan. I'm representing the FS-ISAC and it's more of a question. The question I guess I'm looking at is, "Is there a description of what the analysis process is", right? Because as I look through at the challenge you have, right, there's 23 comments on the docket. There was workshops all over the place, you know, with huge amounts of text available. There's been lots of—there's lots of reporting on what should ISAO metrics look like, you know, maturity models, et cetera. So, I'm struggling a little bit to understand what is the analysis process you're going to use, and is it focused on identifying what those tiers are, or how is that going to be developed?

RICK LIPSEY: The analysis process is still in development, frankly. So, the guys have built a framework and a tool to help with that. I'm certain we're going to evolve that as we go based on the discussions that we have here. To be clear, the purpose of the analysis and the synthesis is to try and make the information that has already been pulled together through previous meetings, and through what we're getting in this meeting, and what we're going to get in the data call accessible, and that it is accessible to the working groups. So we're putting things into logical categories to allow—to be able to provide that in a distilled way to the working groups. So if we have comments on—reflective of ISAO membership: "What are considerations of who should be members of ISAOs? And what types of memberships should we have?", we're going to try to collect all those comments and suggestions and concepts into a bucket that we're going to hand to a working group that is then going to step through the process of developing

statements of principle, policies, process flow diagrams associated with ISAO membership.

GREG WHITE: In terms of the tiers—is that the second half of the question? I was going to go ahead and start talking about that one. We recognize that—I mean, if you take a look at the existing ISAOs that are out there, including the ISACs, we anticipate in especially the comments that we’re receiving from DHS that there’s going to be a tremendous proliferation of entities and organizations wanting to form ISAOs. They’re going to vary tremendously in not only the type of membership, but the individuals—what information they’re going to be willing to share, and so on and so forth. One of the things that we’re working on right now (and I talked to DHS, and we talked to some other folks about, and most likely we’ll have a data call on this as well), is I want to start establishing some use cases. Some descriptions of—can we identify the different types of information sharing organizations that will be created? Can we envision this and—take a shot at trying to envision that and from those use cases that we develop and the different types of information sharing organizations, how will they share information? What kind of information are they going to be interested in sharing? How are they going to share it with the government? Will they not share it with the government? Will they share it with the other entities? So on and so forth. Develop those use cases and use that to help start up a conversation on, “Okay then, now, here’s some different potential use cases that we’ve identified: different types of organizations, different types of information sharing that may take place ultimately. Can we start creating a tiered structure around that?” And I’m not sure if tier implies a hierarchical. I’m not sure if it’s as much a hierarchical as its multiple categories of Information Sharing and Analysis Organizations. So, a lot of work to be done on that. It will also, as Rick mentioned, everything is going to be done in the open. So we’re going to be doing some work and then we’re going to be putting it out there for public comment. So we anxiously anticipate: a) the things that we come up with, and b) what you’re going to be telling us. “Did we miss it? Did we miss the mark on these? Did we forget something? Did we not include something? Did we have a comprehensive set of use cases or did we just not think of some possibilities?”

BRIAN ENGLE: I was just going to join in on that comment. One of the things that was really interesting in the sessions (and I think it’s something that we can definitely consider when we think about the aspect of tiers) is that there were a number of things that were brought about that are sort of questions. And I’ll just take the case of self-certified versus certified: is that an answer to a question, or is there a set of criteria that actually delineates across different tiers? And I think we’re going to have the ability to look at a lot of those types of things that have multiple answers or divergent opinions, and see how they actually fit into tiers of different types of sharing organizations. And that’s just the process that working groups are going to have to go through as they kind of break that down and match those up to the needs of sharing organizations as they either exist in their formation or exist today or as they form throughout this process. And also looking at the existing structures of things like the ISACs and seeing where those types of things are working really well and where we can apply different principles to emerging organizations. So, just to summarize that, I think it’s a really powerful opportunity to take some of these things that we have as questions and not look at them as “Yes/No”, but look at them in varying degrees of, perhaps, maturity, or things that can be tackled in tiers of different types of organizations.

GREG WHITE: And if I can add one further comment on that: this is going to have to be done in parallel with some of these other things. Because we do not want to establish the working groups, have them go off for six months doing a lot of great work, and then say, “Oh, by the way, you need to consider this tiered structure.” So these tiers—we’re going to need to have a skeleton (at least) of the tiers when we form the working groups so they can keep that in mind as they develop the standards, processes,

procedures, so on and so forth.

HEIDI GRAHAM: Alright, so you've been patiently waiting. Thank you.

DAVID TURETSKY: David Turetsky, Akin Gump Strauss Hauer & Feld. What impact, if any, do you anticipate the passage of the information sharing legislation by Congress might have on your work plan, on your definition of groups, on your timelines?

GREG WHITE: Okay, I'll go ahead and jump into that one there. Good question. Don't know. To be honest, we are obviously—we're cognizant of the issues that are going on—the things that are going on up on Capitol Hill. We fully recognize that Congress may pass some bill that may impact what we're doing in this information sharing and analysis effort. And if and when that occurs we will obviously have to deal with it because while we—if you notice the intention here was to not. . . . To go back to some of the earlier diagrams, to go back to the Executive Order: the intent of this Standards Organization is not to create regulations, not to suggest to Congress any kind of bills that need to be passed, not to do any of that. We're separate from that. That said, if Congress comes along and passes some bills related to information sharing, we have to follow the laws. So, they will have to be considered and we'll have to see how that will impact anything that we have done or are doing at that time. If that sounds like I'm tap dancing, yes, because I simply don't know what's going to happen in Congress. Will it pass? We know something's passed in the Senate. What's the House going to do with it? What's going to happen in Committee? I don't know. My crystal ball is too murky to be able to tell.

HEIDI GRAHAM: Sir, before you respond to that, if I may, may I check and see if there's anybody else who would like to speak? And then I'll go ahead and pass the mic back to you.

DAVID TURETSKY: Let me just finish the question.

HEIDI GRAHAM: So, is there anyone else who would like to speak?

[Silence.]

HEIDI GRAHAM: Sir, go ahead please.

DAVID TURETSKY: I was just going to finish up by saying, respectfully, I understand where you're coming from but, respectfully, my suggestion, in the spirit of suggestions and recommendations, would be that you have some sort of plan in anticipation, because you have very tight time tables. There are some pretty momentous things that are included. I don't know what the answer is on what the impact—you know, how to organize the impact. I think it is very, very clear there will be (if it passes) a major impact and so, respectfully, I just suggest that you come up with a plan internally to anticipate that so you'll know what to do. I don't have any specific suggestion for you now. That's all.

GREG WHITE: Absolutely, and I apologize if it seemed if I was being somewhat flippant in my answer. In my other job as the Director for the Center for Infrastructure Assurance and Security, we are actually heavily involved with various congressional offices and know what's going on with some of the bills. So we are tied into—we have our own lobbying folks up in DC for our own purposes and those folks are tied in very strongly with certain offices and so we are keeping cognizant of what's going on, what's being done, what is being said, what's going on behind the scenes, so that we are not caught off guard but I guess we're just not ready to make any kind of statement about how that's going to impact us at

this point.

HEIDI GRAHAM: Alright. Sir, to my left.

KENT LANDFIELD: Kent Landfield from Intel Corporation. My question is we've done this work today. How are you going to communicate with the group in this room going forward? We don't have a website. We don't have e-mail other than one e-mail address (and that was really through DHS, initially). So, when are we going to see some infrastructure around the ISAO Organization so that we can start collaborating?

RICK LIPSEY: Thank you. Excellent question. So that's at the top of my hit list. I would like to have that already in place, but the truth of the matter is we've been focused on putting together the event you've been participating in today. So, building out that website if what's next for us. In the interim, the answer is that we've established the ISAO@lmi.org box. So I'd encourage you to use that. Feel free to contact any of us individually. We have your e-mail addresses through the registration process that we had today. So until such time as we get that web presence—that public presence up and running that's how we're going to do things initially. And the Twitter account. We have the Twitter account.

HEIDI GRAHAM: Alright, sir, you have the floor.

JAMIE CLARK: Good afternoon. I'm Jamie Clark from OASIS which is where the STIX and TAXII standards are being handled. DHS gave us the adoption agency custody over their babies and we're going to try and help bring 'em up. First of all, thank you to all of you for taking this on. A lot of work in 60 days and it's helpful to have some structure for what we're doing. I come from "standards planet", not "beltway planet". And following up on what my friend from Intel said a second ago, let me just mention a cultural issue which I noticed today and has been present in other similar projects. Because this isn't our first rodeo. We did it with SGP. We did it with NSTIC. We did it with ebXML with some of the people in this room 20 years ago. As soon as you can, please move the dialog into dialog. Notice that when the gentleman asked, "How do we communicate with each other?", you said, "You can talk to us by e-mail. Just to us. And we can talk to you." No vehicle for talking with each other. I work for OASIS. If I get up and say, "OASIS wants this. OASIS wants that. OASIS has an opinion. . ."

HEIDI GRAHAM: [Interrupts.] One minute.

JAMIE CLARK: . . . my members will kill me. It needs to be about what the members want and you need to turn that around. Thank you.

HEIDI GRAHAM: You're welcome, sir. Thank you.

RICK LIPSEY: That's a great observation and great input. Thank you. Obviously, it is our intent to create a platform where we can have that type of dialog that we're talking about.

JAMIE CLARK: Hopefully before most of the decisions are reached.

RICK LIPSEY: Obviously! [laughter] It goes without saying, thank you.

GREG WHITE: And through the work groups. The working groups will definitely be a collaborative environment with a lot of information sharing going between the members of the working groups. Not

only is the working group going to be collaborative, we recognize that not everybody will be able to be a member of every working group (or may have the time) and so there's going to be an opportunity for the public to comment on what it is that the working groups are doing as well. So we do want this to be very open and very collaborative. We just don't have all the mechanisms in place right at this moment.

BRIAN ENGLE: I was going to jump in because one of the things in the comments that came out that I think is noteworthy for us to realize is that this process somewhat started with an Executive Order, and it sort of has started today, and then it's going to have another "sort of" start in February. We're in a project now that is going to have people joining mid-stream, and mid-stream is always going to be a new and different place. So, I think it's really incumbent upon the working groups to be able to sort of encapsulate to date and be able to make the things that are sort of reached, not just significant decisions. Because we don't want to have to do another workshop and rehash and capture what we captured kind of things, right? So I guess I'm sort of reiterating for the record here or whatever to make sure that our working groups really think about that process and they think about time capsuling along the way so that people that jump in midstream always have a way of sort of seeing what's been arrived at to this point.

HEIDI GRAHAM: Thank you. Do we have any other comments or questions?

[Silence.]

HEIDI GRAHAM: Okay. I'm going to wait until it's just uncomfortable just so that anybody that wants to share will have an opportunity.

[Silence.]

HEIDI GRAHAM: Alright. Last call?

[Silence.]

HEIDI GRAHAM: Great. Thank you. I'll pass the floor to Dr. White for closing comments. Thank you, everybody.

[Applause.]