

**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.

Initiating the ISAO Standards Development Process

HEIDI GRAHAM: Our last speaker this morning is Mr. Rick Lipsey, the Deputy Director of the ISAO SO. Mr. Lipsey also serves as LMI's senior strategic cyber lead. He served 28 years as an Air Force officer, holding significant operational and general staff positions during his career. Please welcome Mr. Rick Lipsey.

[Applause.]

RICK LIPSEY: Thanks very much, Heidi. Thank you all for making time to be here today. The discussion we're engaged in is an important one and it's critical to our national security. It's critical to our economic security. It's good to see the private and public sector coming together.

So, what's today? Today is 40 for me. The standards organization is 40 days old. We started on the 1st of October and I already get questions about, "So, have you published some standards yet? When are you going to publish these standards?" So, let me share with you where we're at and what we have accomplished in our first 40 days. As Dr. White shared with you, we've developed an organizational structure. We've brought our folks on board. We've gotten organized in figuring out how we're going to do business internally. The other thing: Mike Echols was very kind to host us for a visit a couple of weeks after we got started and he handed me this binder. And I beefed this binder up from even beyond what he originally gave us to incorporate all of the great information that has been collected since the Executive Order was signed in February. So there have been a number of public meetings; there have been comments put into the public record, both through the federal register as well as through public meetings and workshops. And so, this is our reading book. This is our textbook in the standards organization right now. We don't have all of this digested yet. What I can tell you about it is that we are in the process of analyzing and synthesizing that information that's been collected. So thank you very much to everyone who has participated in the process today, you've given us a rich repository of information on a number of important topics and considerations as we look at "How do we build this network of ISAOs and what should they look like?" So, that analysis and that synthesis is ongoing.

We've started the standards development process and we've charted something out that we're going to share with you today. I'll share a little bit of it here. You'll hear more of it in a breakout session that I think is probably at the 75-80% point, but we'd like your feedback on that. As well as a number of supporting documents—so we're working through the specific guidelines and templates and whatnot for each of our working groups, to help them in the work that they're doing and in their coordination and their work with the Standards Organization.

We've begun some initial engagements with the ISACs. Thank you very much to the National Council of ISACs for inviting us to participate in their last meeting. That outreach is going to broaden considerably

over the next several weeks. Candidly, we've been pretty focused on preparing for this meeting and this initial opportunity to have a discussion with you. But look for that to continue to deepen and broaden in the weeks and months ahead.

We've got a number of things that we're formulating and the whiteboards are filling up with good ideas. And we're also working on some supporting structures. So, how do we share information with you? We're going to have a website, but it ain't there yet, so, again, that's an effort that we'll put more energy into after we get out of this initial public meeting, as well as various tools (automated and otherwise) to facilitate the development and evolution of standards and the collection of public comments on those.

So let me take a minute to talk to my friends in the ISACs. Frankly, you all have got this figured out and it makes a very nice model for what we look at and what we aspire to help the ISAO community to evolve into. We have some ISACs that are incredibly mature with very robust and sophisticated capabilities. They're the guys that I think of as the gold standard for what we want. We want to bring those—we want to advertise those capabilities so folks understand they are out there and maybe we have some folks plug into that. Maybe we raise that game—we continue making that better. But we also recognize that even within the ISACs we've got some organizations that function very differently than that. And they have been structured in a way that meets the needs of their constituents. And I think that's critical in what we are doing in terms of putting together standards for ISAOs. And so, step number one: ISACs—we want to take what you've done in your various instantiations and adopt those and use those for the broader community (for those who don't currently have access to that type of information today).

Along the way, as Brian alluded to, there's got to be a little retooling that's going to be done for some of that to allow for some of the different interests that are at play and the other constituencies that are coming out (coming to the table) outside of the critical infrastructure sectors that we've historically addressed. Importantly, as a standards organization, we want to foster a very robust dialogue with the ISACs. We believe your participation and influence in the development of our initial set of standards is going to be critical to our long term success. And, so, take this, please, as—if you haven't heard it before—as an initial invitation not just from me, but from the standards organization writ large, that we want to have a conversation with you, and that we welcome your input and participation in shaping these efforts as we go forward. I'll also foot-stomp a point that Dr. White made: we're committed to not breaking what's working. We recognize that many of you have spent significant time, effort and expense to develop a model that works for you and your members and your constituents. And so, our hope is that we develop a set of flexible, and yet consistent standards that would meet your needs, that would be helpful to you, that would help you, as well, in your practice. But, in no case do we want to adversely affect anything that you have put in place and how you do business on behalf of your constituents today.

So what is it that we're going to try and accomplish today? As Dr. Graham alluded to, we're coming to the end of kind of the introductory, context-setting remarks and we're about to jump into the meat of the day. We're going to do that through a series of breakout sessions. Each one of you has on the back of your name tag a block letter. It says "A", "B", or "C". (It's just a way of conveniently dividing us up into groups.) Through the day, you're going to visit three breakout rooms. Natalie Sjelín is going to be in this breakout room and she's going to be talking about Meeting the Urgent Need. That is, "How do we help find folks who are struggling to get out of the blocks or improve their game today? What are some of those best practices and lessons learned that we can put together?" Brad Howard is in 1 South A which

is diagonally opposite of us over here, and he is going to be leading a session on the framework of standards. The “What”: what is it that we’re going to be producing here over the next few months and years? And then, Daniel Knight is going to be in 1 South B and he’s going to help lead a discussion about the standards development process that I alluded to. “How are we going to this? How are we going to form the working groups and do that work?”

Here’s the quick thumbnail preview of what you’re going to see in those breakout sessions. When Brad is talking about the “What”, we’re talking about, “What are the standards that we’re going to develop?” So, we’re going to clear the air on a vocabulary question, to begin with. To some folks, the word “standard” has a very narrow, specific, and limited meaning. We are using the word “standard” in a much broader sense: that is, to encompass anything from general statements of principles, to policy documents, to process flow diagrams, all the way down to specific data standards. So, we’re looking at that broader understanding of the word “standards” here as they apply to ISAOs. Those standards or products are written about a series of topics, so the topics we’re going to talk about are: the capabilities of an ISAO—what does it mean to be an ISAO? What are the minimum thresholds of capability before you can wear that label? What do we want to say about members and who is allowed to be a member and who isn’t allowed to be a member? How are we running these things as organizations? How do they operate financially? What are the legal considerations? How are we doing minimization, or otherwise protecting the security and the privacy of information? So those topics, building that topic list (or what I refer to as the “Table of Contents” for the big book that we are going to publish as a Standards Organization), that’s what Brad’s going to be talking about in 1 South A.

In 1 South B we’re going to talk about the “How”. So, Daniel Knight is going to help with the discussion of the process and how does this work. This is our diagram that we have come up with that, as I said, I view it as probably an 80% solution on how that process is going to work. So, based on the information that we’ve collected about the topics that need to be developed and the analysis of the information that has been gathered through previous workshops and meetings, we’re going to go back and formulate some logical construct of working groups that seems to make sense. The ISAO SO will charter those working groups and work with you all to develop leadership teams, to staff those and put those together and then we’ll look for the working group then, to publish an initial request for comment: “Here’s our working group. Here’s what we’re going to be talking about. Here’s our initial thoughts (if any)”; and we put that out in the public domain to solicit some inputs on that.

Based on that, then begins an iterative process of actually writing those various documents: the statements of principles and the policy documents and the process flow diagrams and the templates and whatnot that are evolved through an iterative process within the membership of the working group, also informed by the core of the Standards Organization (and we will reach out to other independent experts as needed to support those working groups) that are then ultimately published. More details on that when you get into Daniel’s session, but that’s what you’ll talk about in the second breakout. And then in the final breakout session, Natalie, in this room, is going to try and address “What can we do to meet the need today?” If the need is urgent, if it is compelling, and so what are we doing to help the entire spectrum of sharing organizations? From the Southeastern Michigan Dollar Stores, who have said “Gee, we want to form one of these ISAOs. We’re not even sure quite what it is or how to do it”; all the way up to someone who might be as mature as, say, the FS-ISAC. How can we help bring that game up? So, those are the things Natalie will be talking about in here.

Here’s some general principles about how we believe as a standards organization that we need to conduct ourselves in this meeting and in our future deliberations going forward. In everything that we’re

doing, there's openness: that means anyone is welcome to participate in the process. Transparency is important: nothing is getting done in a closed, smoky room, but it's open to the light of day. Consensus-based, which means we bring together that general understanding of what is best for the community as a whole. It takes into account a balance of interests. We are going to have—we each bring individual perspectives, and we each bring individual issues to the table. Again, the goal of our process is to figure out, “How do we accommodate those specific issues and concerns in the broader context of the goals that we’re trying to achieve?” We’ve heard several times, “Everything that we are doing is voluntary”. We’re trying to develop a series of interlinking, interwoven network of partners and communities all under the understanding that we’re going to do no harm.

So, let’s take a breath for a minute and get real about how we’re going to do this. This is not an easy task. Scaling world-class capabilities (I believe that’s some of what we have developed today) is not easy. There are a lot of considerations to be taken into account. There are diverse interest groups that we’ve alluded to, and so, to accommodate that, the standards that we develop have to be consistent but flexible. What do we mean by that? When we say they are consistent, that means that the standards need to be internally consistent and they need to be linkable: we should not have conflicts that are expressed in the standards that we develop. However, they have to be flexible. This is not going to be a “one size fits all” solution. Not every individual standard document that we create is necessarily going to be applicable to every single ISAO. To the extent that we think about tiered or multiple models of ISAOs, there will be a family of documents that might apply to one group of ISAOs, and a slightly different family of documents that apply to another set of ISAOs. But between them, they should be consistent to foster this integrated network.

One of the points I want to foot-stomp is that the need for us to undertake this effort and the need for us to be successful in this effort is vital to our economic security and our national security. We have challenges that we’re facing today. As you in this room know, those challenges continue to grow by day. So tools that used to be accessible only to nation-states are now readily accessible to anyone who’s willing to write a check and pick up capable tool sets. And to that extent, I say, “Perfect is the enemy of good.” There are issues that we could debate until the cows come home and yet they may not have a major impact on the outcome of what we’re doing here. So, we need to take those into account, but frankly, we need to move forward.

On the flipside of that discussion, we’re not going to figure out all of the answers today. DHS has established this notionally as a 5-year effort. And, so, we’re going to do the best that we can to move along in a very timely way to accomplish something meaningful in a short period of time, but we’re not going to get it all done in one day. So, that’s important.

The thing that I will ask you all to bear in mind through your discussions in the various breakout groups today, as you are engaging Dr. White, and Brian, and I, and other members of the team today, is to remember why we’re here. We are here for a very important goal of improving the Nation’s cybersecurity posture. By making our nation’s businesses, whether they’re multi-billion dollar giants, or they’re Mom and Pop’s Diner in Phoenix, to make them more secure. We’re trying to help broader organizations improve their posture, no matter where they are on that spectrum of resource and sophistication. I’ll remind you that this is not the first time our Nation has faced this type of challenge: where there were considerable policy and technical issues at play, but in which we were undertaking something that was truly important for the good of the Nation. So I’ll ask you to remember that analogy.

[Recording plays of Kennedy’s challenge to organize and work together to land a man on the moon.]

We're not putting a man on the moon, but what we're undertaking is of similar importance. That challenge was made in the face of a very significant threat to our Nation, and that's where we're at today. So, I thank you all very much for your participation and for joining in this national civic dialogue.

We're going to take a break now until about 10:00 and we're going to go to breakout rooms. If you would, take a look at the back of your badge, that will help you key on where to go. If you've got an A on the back of your badge, you want to be in this room. If you have a B or a C, if you would proceed to the opposite corner of the room, diagonally and meet up there. We'll join back together in a group session later this afternoon. Yes?

[Mr. Lipsey accepts a question from an audience member.]

The five years was the term of the grant that DHS offered. I certainly don't see this as a five-year effort; that was just the term of the initial grant. Thank you.