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.

The ISAO Standards Organization: Mission and Principles

HEIDI GRAHAM: Please welcome Dr. Gregory White, executive director of the ISAO Standards Organization. Dr. White has been involved in computer and network security for nearly thirty years. He's an expert in the area of computer network intrusion detection. Dr. White is a thought leader, an educator of the highest caliber in the classroom, establishing information warfare laboratories, national competitions, and cybersecurity exercises. Ladies and gentlemen, Dr. Gregory White.

[Applause.]

GREG WHITE: Good morning. I appreciate the opportunity to be here this morning. I'm honored to be here with all of you. The purpose, just to start things off here, the purpose we see of this meeting is two-fold, very broadly. One of the objectives is, very simply, to introduce ourselves to you folks. This Executive Order 13691 has been out for several months now. Everybody here is well aware of it; everybody here is well aware of the standards organization that was to be formed; and we wanted to introduce ourselves to you, so you all know a bit more about who we are and what we believe our mission is going to be as part of this development of these standards. The other purpose is to then, again, to continue with the solicitation of comments from you folks. We recognize that there has been a lot done prior to the announcement of the team as being selected for the standards organization. We are cognizant of that information that has been already provided and the different meetings that are out there. We are taking a hard look at it. We are not going to ignore any of that. We're not going to duplicate any of that. But we want to start engaging directly with you as a team.

The team (referred to it a couple times and was mentioned earlier) consists of basically three entities: the University of Texas at San Antonio Center for Infrastructure Assurance and Security (the CIAS); I'm the director for that entity, but the other two partners are LMI, whose facility we are all in today. And I'm personally very thankful for that partnership and for LMI because one of the requirements for the grant that we received was to have our first open forum within 45 days. We would not have been able to accomplish that without the tremendous work of LMI and the staff here. It's a beautiful facility and hope everybody has an opportunity to wander around a little bit, just to take a look at it, at the building, at the facility. The other partner that we have is the Retail Cyber Intelligence Sharing Center, the R-CISC. We're excited, collectively, to be selected as that standards organization, the Information Sharing and Analysis Organization Standards Organization. That's the last time I'm going to say the whole thing. It's the ISAO SO, if you will.

You're going to be seeing and hearing people refer to that Executive Order 13691. It's been out for a while—since February. It's the thing that got this whole, this specific team and organization rolling, and I know that there's a lot of questions. We've already fielded a number of questions from various organizations: specific entities out there already conducting information sharing and analysis operations; from the media. There's tremendous, I mentioned, there is a tremendous interest in it, and so one of the things I wanted to convey to you folks today, also, was that we're aware of some of your

concerns out there and maybe you start, I'll mention a few of them and hopefully allay some fears in some folks, especially that we've seen in the media, have misconceptions about what it is that this ISAO SO is supposed to be doing.

The first one up here, and if you notice we have it highlighted in red twice: "Voluntary". We understand. We get the message. This is to be a voluntary operation here, individuals. You'll notice there are two aspects to the voluntariness, if you will, of this effort. The first is that a voluntary formation, there's not going to be any requirements for folks to go out there and to form ISAOs. It is a voluntary effort. And the second one at the end of this, if you notice, it said, and the Secretary mentioned this. She said (and I'm going to paraphrase what she said, but as I heard it) that she desires, and the government and we desire that people will share information with the federal government (with the NCCIC), but that was a desire. That is not a requirement. It will be voluntary. There's a concern out there some folks (just simply, to be quite honest, and we recognize it) may not be comfortable at this moment with sharing with the government, and they're not going to be forced to if they do not want to. They will be encouraged, but it is voluntary.

We are all—everybody here is aware of it: there is a cyber threat to this Nation. That's what we're here trying to address. There are many aspects to the defense of the Nation from the cyber threats, one of which is information sharing. And that's what we see as our mission. That's our job here. It's to address that information sharing aspect of the solution to the threat, the cyber threat that is posed to this country. And our vision, then, very simply, is a more secure nation based on that information sharing aspect of addressing of the cyber threat.

Looking at the Executive Order, once again, the goals, notice if you go back to the Executive Order, take a look at what is the purpose of this ISAO SO. What are our goals? We're supposed to be trying to encourage (and we will) going to encourage the creation of a number of different ISAOs. We have a lot out there already, but we anticipate that number growing tremendously. I hesitate to use the word "exponentially", but it could very well be that. In the next year, 2 years, 3 years to see a tremendous increase in growth in the number of the ISAOs. We want that to happen. We want to encourage that. So that's going to be one of the things that we're going to be doing.

The other thing is, once again, notice that voluntary set of standards once again, and there's another term in there that's important and that was mentioned is "certifying". If you notice it is self-certification is what we envision at this point, so that entities out there (and I fielded a number of questions about "Well, what about all of those entities out there that are already referring to themselves as ISAOs?"). That's okay. We'll have a self-certification process that will be identified (will be developed) as part of this overall organization and the process. We will address the voluntary aspect of that and some other concerns we're going to be addressing: some principles, guiding principles, trying to allay some fears.

One of our very first, and possibly the foremost one is, "Do no harm". Our intention as we develop these standards is not to dictate to any of the current Information Sharing and Analysis Organizations that are out there. If you think chiefly, a large portion of those, being the ISACs, which have been in existence for a number of years doing a very excellent job at sharing information in their sectors that they have been developing and between each of the ISACs. We don't want to come and our intention is not to go and to start dictating to any of the ISACs how they should be doing their business. We're not going to try to, in other words, 'do no harm'. We're not going to try to change any of the robust processes or procedures you already have in place.

Consensus-driven. That's why we are all here today. This is not going to be the ISAO SO going off in a corner somewhere behind closed doors developing some standards and then posting them and saying "Here's what you need to be living by, folks". We're not going to do that. This is a very open, public consensus-driven effort. We want to hear from you folks. There's a lot of tremendous work that has been done out there. There has been a lot of work since the Executive Order was implemented, well, not implemented, but, announced. There have been a number of different public forums and public meetings. We're going to take into consideration all of the comments that have been provided before and we hope will be provided in the development of the products that will come out of the ISAO SO. Once again, we are going to concentrate and to foot-stomp that word "voluntary", once again, because that is very important. We recognize how important that term is to this overall effort.

If you take a look at what we anticipate producing, if you go back to the Executive Order, again, there is a number of different things it mentions: obviously, standards. Standards is one of the primary things that we're going to be talking about and we're going to be developing and we're going to be working on. But, there's some other terms that were in there: standards, guidelines, templates, and we intend on producing those, developing those, as well, with the idea being as we try to promote the creation of ISAOs, entities who may want to stand up an ISAO, they may have the desire to do it, but the question may be, "Okay, great. What do we do? What's the first step?" Well, instead of handing someone a bunch of—well, here's the standards: go forth and implement your ISAO. We want to be able to try them with templates. Here's how you get started. Here are the kinds of things that you need to do. Here are the standards that you can live by. Here's some guidelines that you can use. Here's some other best practices that have already been developed out there and are in use by other Information Sharing and Analysis Organizations. We're going to be gathering all of those things, putting them together, in an effort to try to help new entities develop Information Sharing and Analysis Organizations. The desire is to attempt to standardize across all of these existing best practices, procedures, policies, and so on and so forth.

We recognize that this is not just about the ISAO SO. As I mentioned, we're going to emphasize it again and again, we recognize that there's a lot of great information sharing going on already. A number of very developed entities out there in existence with very robust processes and procedures in place. What we want to do is to be able to draw from your experience. When we—using the ISACs as an example—if we can go to each one of these ISACs, talk to them, and find out that there is a common best practice that every one of them is using, probably that's a good thing that a new ISAO that's being formed ought to consider. It may be, if it's applicable to every other Information Sharing and Analysis Organization in creation, then—in existence currently—then any new ones being formed probably ought to consider that as well. We want to gather that information. What are the common things? Whether they be protocols, processes, procedures, guidelines, templates. What are they that are currently common amongst the Information Sharing and Analysis Organizations in existence? Let's identify those and get those out there so that new ISAOs who are wanting to be formed and new entities wanting to form an ISAO are able to use them and get a head start so that they don't have to learn some of the lessons that others have already learned the hard way.

How are we going to do that? This is, just very roughly, our organization. I'm the executive director, as was mentioned, but we're going to have three entities in that organization. The stakeholder engagement side, most of you have—hopefully all of you—have met Mr. Rick Lipsey from LMI, he's in charge of our stakeholder engagement portion of it. Dr. Keith Harrison—who unfortunately could not be here today, well, to be honest, because he is in Amsterdam conducting a cybersecurity competition (Black Hat Europe) right now—he's going to be heavily engaged in the lifecycle management, the

standards lifecycle management portion. And Ms. Natalie Sjelin, who some of you will have the opportunity to meet today—hopefully all of you will have the opportunity to meet as well, because she is going to be moderating one of our sessions—she's in charge of the ISAO support portion. But, once again, as was mentioned, this is not just about the ISAO SO going off in a corner somewhere and developing some standards—you know—blindly. What we envision are a series of very active working groups with very active leadership teams among those who are going to be providing input into those standards, best practices, policies, guidelines, and so forth. And, in addition, individuals who may not either have the time or the inclination to be a part of the working group, but may want to provide public comment, we're going to be open and provide mechanisms to do that as well. You will hear more about the formation and how these will work, but Mr. Lipsey will talk about some and we'll also be talking about some of these in the breakout sessions, so I'm not going to go into any more detail right now, other than to say, once again, this is not just about the ISAO SO. This is about you folks participating in working groups to provide us the information and the collective wisdom that you have already acquired so that we can move forward in the development of the standards, guidelines, templates, and so forth.

Roughly (we're not going to go into great detail in this diagram either here), but those three different entities that I mentioned before in the ISAO, roughly equivalent to the three things that you see here: the stakeholder engagement that Mr. Lipsey is in charge of. His job is to go out there and to beat the bushes and find all of you. So far, he's done a pretty good job getting all of you here today, but he's going to continue to engage with you people to make sure that we're receiving the comments, conduct surveys, find out how we're doing. His job is to interact directly with all of you and those individuals who should be here today, but may not have known about it or were not able to be here or whatever. That is his job. Dr. Harrison's job is going to be to work on the development of those products that will be produced: the standards, processes, procedures, templates, guidelines, and so forth. Ms. Sjelin's job is going to be helping ISAOs develop. She's going to be going out there and when some entity or group of individuals wants or decides to come together and they want to form an ISAO and they say, "Okay, how do we do it?", she's going to be helping them. She's also going to be working with you folks in terms of any other support or anything that we have that we may be able to provide you—existing ISAOs—as well.

I'm going to, I know I have said this before, but I can't over emphasize it: it's not about us, it's about <u>all</u> of us, including and a major portion of that 'us' is you folks. The entities that you're already part of: the Information Sharing and Analysis Organizations that are already in existence out there. We want to learn what those common elements are among you folks, currently, so that we can use those to help new entities form. That's what we want. We want that public comment, we want that information. This is consensus-driven.

Now, the plan, just to give you sort of a feel, I had a lot of questions about how things are going to move forward. Here's our tentative—underline that word—idea about what is going to transpire, what are we shooting for, what are we hoping to accomplish today, in the next 60 days, and in the next year. Today, obviously, the first public forum. There will be four public forums that will be held ultimately. We're going to be issuing a data call within a few weeks, in two weeks here, and we're going to have that data call and it's going to be open for 60 days. What we are going to do is we are right now forming some of the questions that we want to ask for you folks to provide comments on, what the information we see is valuable to not just us, but, to those working groups that will be helping us develop the standards, guidelines, templates, and so forth. In terms of the working groups, within the next three weeks we want to obtain suggestions for 'Okay, what working groups?' We're going to be discussing in some of the breakout sessions today, one of the breakout sessions is going to be talking about the various working

groups, so you'll hear more about that today, but, just to give you a feel for our timeline, within 21 days we would like to listen, not just take your comments today, but if you go back you think about it and say "I should have said this", or "Here's a new idea I had that just popped up", or "Something occurred to me", that you have an opportunity to provide comments on what are those working groups. What should they be? What are the ones that we should be forming?

The framework of standards (standards framework) and the process that we're going to be going through in the development of these standards: you have a flier that has a nice diagram that's going to be explained a little bit more. Mr. Lipsey is going to be talking about that some more and will discuss more in some of the breakout sessions, but that's being presented today. The minutes from today's session along with the transcripts, the audio transcripts will be posted within three weeks so if anybody wants to go back and listen to themselves or listen to what's going on, what's been said, or if you know of individuals who are not able to be here but would have liked to have been here or just want to know what went on, that information will be posted. Once again, the intention is to have this be a very open process.

Within 30 days, we want to form the initial—at least the initial—working groups. We want to start taking names and to start identifying individuals who will be on the leadership teams. More on this to follow. But just to give you a time frame, we're going to need to form those working groups very, very quickly. Then, in 60 days, we're going to have that—as we mentioned—we're going to have that data call. We're going to ask for comments to be provided within that first 60 days on the data of the different questions that we had the things we're going to be asking for some input on. We'll leave the comment open afterwards so that if someone comes along later and wants to provide comments that's great, but, basically at that 60-day point we're going to cut it off and take all the comments that we received at that point and use them and run up to our second open forum, which will occur sometime before 13 February in 2016. Probably the last week of January or the first week of February. In the first 60 days we'll also announce who the working group—what the working groups are, and the leadership teams who the chair is for those, each of those individual working groups. So the working groups will be formed. Then, after that, before 13th of February—the reason the 13th of February—that very specifically is the one year anniversary of the Executive Order. So, here's what we would like to accomplish within that first year, if you will, of the issuing of the Executive Order. So, we're going to have the first meetings after the working groups and the teams have been identified, we are going to encourage that the working groups have their first meetings. That will be a teleconference kind of meeting, most likely not in place, because we anticipate individuals from around the country wanting to participate. We'll have our second public forum by 13 February, either the last week of January or first week of February. That second one will be in San Antonio. More information on that to follow. It will be posted and what will be the focus of that second forum. Yes, ma'am?

[Mr. Gregory White takes an audience question.]

GREG WHITE: The question, if I understand it, is "Are we going to"—for these folks in the other rooms who may not have been able to hear the question—the question was "Are we going to in some way, shape, or form, bundle the information up that's provided here or subsequently that will be provided to us come up with some sort of method or mechanism, whether it be Federal Register or some other mechanism to get the word out to those individuals who may not have been a part of this today, or who may not know about it?" Yes, absolutely, as a matter of fact, that is a key element of this, is getting the word out. That's what Mr. Lipsey's whole job is. It's to work with stakeholders, both the ones we currently know about as well as stakeholders that should have been here, individuals that should be

participating in it, but may simply not have known about it. And not just in providing information on past forums, past conversation, past public comments. I'm going to go ahead and press on. We've got to get ahead to our other ones. I'm not trying to cut anybody short here. I will be available for comments and questions in a bit, but we want to keep this thing moving so we can get on to the breakout sessions, because the breakout sessions is where you folks get to provide your comments. That's where we're going to be, basically. I'm going to go ahead and just, if I may…

[Mr. Greg White accepts another question from an audience member.]

GREG WHITE: The question was, "Is there going to be an ability to provide comments on the timeline?" This timeline—once again, I mentioned was tentative. Absolutely, please provide comments. It's going to be—and Rick is going to be talking some more about this—how can you provide comment? Not just on standards, processes, guidelines, or anything that is going on, but anything that we mention today. Absolutely, we love to have comments. If you see something that we tentatively said we think we would like to do the following by a certain amount of time and you say "That's just not going to work. That's unrealistic. In our experience, or in my personal experience or whatever it may be, we think that this is—you're not providing enough time for comment" whatever your comment may be, absolutely. We will want that. Rick will be talking—Rick is going to be coming up here. We have two more briefings here before we get into the breakouts. Rick is going to talk about, how, a little bit more about the organization, the processes, the procedures, and we'll be talking about how do you provide comments on anything about this process. Absolutely. I don't mean to be cutting anybody off, but I do want to provide them the opportunity—like Rick—to provide the opportunity to talk about it in one briefing. "How do we anticipate getting comments?" So, absolutely, we do want comments. Absolutely, we are open to this whole idea and this is not. . . . As I mentioned, the term was "tentative". We recognize that this is just our initial cut at what we would like to have. This is our goal. Let us know: is this unrealistic? If it's not realistic, let us know. We want to benefit from your experience and the knowledge that you have in this area.

The third front public forum is going to be somewhere to be identified on the west coast by the time we have the second one, we hope to have the date and the location nailed down. Right now, to be quite honest, we don't have a location, don't know exactly where. We have some ideas about where we think we might like to have it, but it has not been identified. But we will have that by then.

And then the last slide here, once again, and there I've actually stuck it on the slide on this one, "tentative", but here is what we're trying to shoot for. "Will we make it?" Good question. "Is it realistic?" We'd love to get your comments on that. One of the things that I—on a previous slide there, that I didn't emphasize as much—we anticipate (and we'd love your comment on this, and we're going to ask for it); we believe that there's not going to be a single standard for what an ISAO is. Because there are many, many different types of organizations out there. There are many different desires in those organizations as the Secretary mentioned earlier, some may want to participate with the government and provide feedback; some may not. So we anticipate—fully anticipate—we do not have this fleshed out, we have some thoughts and ideas. We would welcome your thoughts and ideas on it, but we envision a multi-tier set up of some sort, so there will be different tiers of ISAOs. Each one of them—for example—maybe the ISACs—the very robust, very well-established ISACs who have tremendous information sharing going on currently and tremendous relationship with the government. Maybe they are a tier four. But then you may have some small retail entity that—ISAO—that's made up of a handful of organizations that may not have the ability to do the things that the ISACs are doing. Maybe they are going to be a tier one, and you get the idea. There's going to be multiple types of ISAOs, multiple tiers,

and within those tiers, we envision potentially different levels. Because on day one, when I declare, "Hey, I'm a new ISAO", are you going to be the same a year later? Or will you start off establishing certain things and then over a period of time you will establish other things? Working through, for example, levels. If you recall, one of the things that we want to be producing are templates. Here's how you develop your ISAO, here's the first step, here's your second step, here's your third step. So that's what we envision. This will be open for public comment as well. We would love to hear from you on that concept.

You can see some of the other comments on the other things we're going to be looking at. We're throwing it out—this idea—this process of throwing something out for public comment, seeking public comment. After a certain period of time, bringing the comments together and then releasing drafts, is what we're going to be doing over and over again, for each one of our things.

Our third public forum we hope to have on the west coast somewhere towards the end of March. We want to have the working groups by then, very well-established and hopefully working hard at establishing those initial standards. We recognize this is somewhat aggressive. We understand that some of these working groups may be large. Rick will talk about this some more, of how this is going to work, but if we want to. . . . There are ISAOs—as you well know—there are ISAOs forming. Mike Echols can talk about it. There are ISAOs forming right now and it could benefit from the knowledge that you folks have. We need to get some stuff out there as soon as possible to help these people. We need to develop the standards as soon as possible. So we are going to be a little bit aggressive on this.

The fourth public forum: location to be determined and date to be determined, but we want to have that somewhere in the summer timeframe. You can see when we're hoping to have the public comments on the initial draft standards out, posting, asking for comments and we hope to have it received by within, basically, a year from when we were established on 1 October. We would like to have at least the initial set of standards published. We do not see that as the end of the job. We don't think we'll have all of the standards developed. We don't think those are going to be the end-all be-all, necessarily. Might they need to be modified, adapted, changed? Of course. For Heaven's sakes, we are in an information technology field, which is constantly changing itself, the standards will need to adapt as technology changes. We recognize that. We understand that. We will have the mechanism to do that.

Bottom line, once again, here are the individuals that are going to be the leadership team. I mentioned the individuals already, including Mr. Engle, who is the Executive Director for the R-CISC. There's e-mail, Twitter (we established a Twitter account so we can get the social media going as well). At this point, I'm going to go ahead and step off. I've gone over a few minutes. I apologize, Rick, for the time. But, to turn it back over to you folks, I will be around all day, I am open to talking to anybody, answering any of the questions that you may have, but we're going to go ahead and move on so that we can get to the breakout sessions, which is where you're going to be able to provide the comments. Thank you.

[Applause.]