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.

DHS's Commitment to a Public-Private Relationship

HEIDI GRAHAM: Our next speaker is Suzanne Spaulding, Homeland Security's Under Secretary for the National Protection and Programs directorate. Ms Spaulding has spent 30 years working for national security issues for both executive and legislative branches, as well as the private sector. Her work in the national security domain spans issues on terrorism, weapons of mass destruction, homeland security, and most relevant today, cybersecurity. Ladies and gentlemen, the Honorable Suzanne Spaulding.

[Applause.]

SUZANNE SPAULDING: Thank you very much and thank you for giving me a few minutes this morning to help kick off this first public meeting of the ISAO Standards Organization. (I keep wanting to say *eye-say-oh*, but the White House says it's *eye-sao*, so. . . .) I really appreciate LMI's hosting of this conference today. Obviously, very appreciative of the University of Texas San Antonio's lead in this effort. Thanks to the Retail Cyber Intelligence Sharing Center for their key involvement in this, but most importantly, I really want to say thank you to all of you. I want to echo Nelson's comments about the kind of civic duty that is reflected in your presence here today.

The key to this process is your involvement and your insights. This is intended to be a very inclusive and collaborative process that really captures your insights and your wisdom for the common good. Your willingness to be here today to contribute is really outstanding and we're very much looking forward—I'm looking forward—to getting a debrief at the end of these conversations and I appreciate the way that you've structured the conference to allow maximum opportunity for real conversation and real input and not just listening to people talk through the day, but, to actually hear from the folks who are out there, engaged in this activity.

You're going to—so you're going to hear from Mike Echols at DHS who's going to give you some specifics. I want to just spend a couple minutes this morning providing perhaps a broader context in which we look at this effort. We're really very excited about this because it is a critical part of our overall strategy to continue to find ways to move that—to use that public-private partnership in ways that go beyond that slogan and actually have an impact and make a difference and in this case, most of the focus I think of our discussion today will be on how to have a real impact on cybersecurity, but I'm going to touch on a broader context that I want to challenge you with toward the end of my remarks.

Key to this—we all know—a really important part of this is data. And so, a key objective for us at the Department of Homeland Security has been "How do we play a role in helping to broaden information sharing and increase the speed of that information sharing?" So, we have had underway an effort to automate information sharing. As a result of that, we have worked with others in the community to develop a set of standards of structured language, STIX and TAXII, a way of transmitting that structured language as a way of understanding and sharing cyber threat indicators. We just launched—at the end of October, beginning of November—that program—that the president asked us and our secretary

directed us to have it done by the end of October—an automated way of sharing this information with our interagency partners at the federal level. We look to share with state, local, territorial, and tribal. And, of course, we want to share with the private sector, and this is bi-directional. The idea here is to have a network of networks so that when malicious activity—when something is detected by one—it can be shared with all to respond and put in ways to protect against. The vision here is that the adversary, perhaps, will be able to get away with something once, or at least try something once. But if we succeed in this, we will stop what we see today, which is where the adversary can just reuse and reuse and reuse and reuse. The idea here is we've got to get faster at detecting and then protecting everyone, and we want to do it at machine speed. So that's the automated information sharing. And ISAOs are a key element of that network of networks.

And so you saw that when the Administration put forth its proposal for cybersecurity information sharing, focused on sharing cyber threat indicators, that ISAOs were a key part of that. So the Administration put forward a proposal and versions of it have passed now in the House and in the Senate and we're moving toward conference to provide—to incentivize—private sector information sharing by providing liability protections. And it was a very conscious decision to not just provide those liability protections for sharing with the government, but also for sharing with each other through these Information Sharing and Analysis Organizations. The decision was sharing this information is the most important aspect of this. Yes, we'd like that information, obviously, to come into the government, into the NCCIC, our National Cybersecurity Communications Integration Center, but the most important thing is that it gets shared. So this is not just a centralized model where everything comes into the center and then goes out to everyone, it really is envisioning this network of networks. That's, again, why you all play such an important role.

The legislation—the proposal by the Administration—did want to incentivize sharing with the government and so to make it easier for the private sector and to allow the government to connect the dots, the decision was made we should incentivize this new incentivize program this information to come into one place, so that it's not in disparate places throughout the government, such that in the wake of some significant cyber incident, that post-incident inquiry finds that we had information in various places that if we brought it together could have prevented something bad from happening. Instead, let's incentivize it to come into one place. If it's going to come into one place, where should that one place be? The decision was the NCCIC, which is the place in the government that has the mission of sharing information with the private sector and getting it out as quickly as possible and as broadly as possible. The NCCIC is not law enforcement, it's not intelligence collection, it is about network defense and collaboration and getting information out quickly.

We have an outstanding record on privacy; we've got the first statutory privacy officer in government, still maybe the only statutory privacy officer in government. So we have worked with our interagency partners, with our office of privacy, our office of civil liberties, the law enforcement and intelligence community, all of our interagency folks to develop the architecture for this automated information sharing so that, when Congress passes this legislation, to incentivize this, we are ready—ready to get that information in near real-time and get it out in near real-time with appropriate privacy protections. So, that is the path we're moving down, and that's why I'm so excited that this organization is standing up and moving out because part of making that work is opening that aperture for Information Sharing and Analysis Organizations.

Existing ISACs, Information Sharing and Analysis Centers, that are primarily built around those sixteen critical infrastructure sectors are key—absolutely vital—key players in this, and are the exemplars. They

will be key contributors to the development of that template for what does an effective Information Sharing and Analysis Organization look like. So, we're looking to those experts to play key roles in this process and to continue to be key interlocutors with us going forward. But we also recognize that there's no "one size fits all" with this and, as I said, our key goal is to encourage sharing of information in whatever groups people are comfortable sharing that information. And we know there are informal information sharing groups today, but we would like to put some regularity, a little bit more formality around those, in part, so that people who aren't yet part of an Information Sharing and Analysis Organization can have some assistance in determining either how to set one up or which one to join; how to assess them. How do I evaluate this? So that is a key role that we're looking to all of you to play.

We are also going to contribute, in addition to this network of networks, sharing that information, cyber information, through automated, through standards that allow machines to talk to machines, we are also contributing information, threat and vulnerability information from those systems we have in place on the .gov. So, at DHS NPPD, the organization that I lead, as you know, in addition to having that overarching mission of protecting, strengthening the security and resilience of critical infrastructure and that interaction with the private sector, we have the lead for the .gov cybersecurity. Departments and agencies are responsible for ultimately for their cybersecurity, but we play a key role in providing some baseline, both in terms of technology in sensors but also information and best practices and the like. So, that information that we are gathering through EINSTEIN (our sensors at the perimeter) and through our continuous diagnostics and mitigation, which are the tools we are giving agencies to monitor the health inside of their networks with dashboards and certain levels of data coming back into us, as we develop that information we are going to put that into this system as well and get that out as quickly as we can to benefit all of the participants.

My cyber deputy, Dr. Phyllis Schneck, describes this as—you know—this use of data and bringing all of this data together to make sense of the world in which we're operating as "the weather map". She has a background and used to work in that field early-early in her career, and when she got here and started looking at all the data that we potentially have access to and the sophisticated analysis that could be brought to bear there, to help us sense and predict more quickly, see more rapidly what is coming at us, she has likened that to the advances we've made in that weather field and that weather map. That gives us some warning; it gives us as a sense of the world in which we're operating. I think it's a really apt analogy.

So the work that you all will be doing today, and in the weeks and the months ahead, is going to be critical to helping us both broaden that information sharing, but, also, enhancing the speed with which we share it, which we know is critically important. As I said, I want to put one challenge on the table for you, and that is, as you're thinking about this, as you're looking at what should these organizations focus on and what are some of the key issues they ought to address, I would ask for your help in the effort that we have ongoing, to make sure that we are not operating in stovepipes around cyber and physical, but that the work that we're doing reflects the increasing convergence of cyber and physical. The evidence of it is rampant whether it is the Internet of Things; the acknowledgement that cyber attacks obviously can have significant physical consequences; physical events can have an impact on your ability to, for your ICT to function; physical security—if you don't have access controls on the doors to your server room; and cybersecurity of your physical security, including your surveillance cameras and your access sensors, et cetera. So, in so many ways, across that entire risk management spectrum, we see that convergence of physical and cyber. I'm engaged in a major effort with my colleagues at NPPD to make sure that we are breaking down stovepipes around cyber and physical, and creating institutions to facilitate that cross-domain, if you will, analysis approach to risk management and I would ask you to

keep that in mind as you go forward.

I would encourage all of you to robustly support the work of this organization and the development of these standards, and to, if you're not already a part of an intelligence or Information Sharing and Analysis Organization, to seriously consider joining those organizations and get your trade associations to do the same. It's really important that we have this robust network of networks if we're going to match the adversary in speed and breadth. Our goal is that every country and the United States has the opportunity to benefit from the cybersecurity information that any of us has that can be brought to bear, either directly from DHS through an ISAO or through a commercial service provider. However that happens, the key is that we've got to have these mechanisms in place to get this information out very quickly. This conference is a key milestone in that effort and I just want to thank you again and wish you luck in your discussions. Thank you.

[Applause.]