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.

Our Progress Towards a Better Future

HEIDI GRAHAM: Next, please welcome Mike Echols, the director of the Cyber Joint Program Office at the Department of Homeland Security. Mr. Echols has asked me to make his introduction short and so I will take him at his word, and without further ado pass the podium.

MIKE ECHOLS: Good morning, everybody.

[Audience responds 'good morning'.]

MIKE ECHOLS: I am very glad to see you all. We've come a long ways in a very short period of time and it shows the power of public-private partnership. I would be remiss if I didn't think the National Council of ISACs and some of the existing ISAOs such as ACSC, High Trust, NCFTA, PRISM, and all the individuals that have participated in the work thus far, that has gotten us to where we are right now.

I'm a guy with a sports background. So, I wanted to talk to you today the way I would talk to any team that I was a part of. I've taken a level of leadership. The team that won the standards opportunity, we are proud of them. The competition was stiff, and we believe that they are going to do a fantastic job in leading the rest of us to this foundation that is required for us to meet our cyber challenge. So, I'm sort of a zealot at this. I really, really believe that this is foundational to us moving forward, and getting past all of the rhetoric. But I wrote down some notes to kind of keep me in line.

Clearly, our ability to identify, debate, and reason to a world-class solution is derived from previously unforeseen partnerships that we've had that allows us to come together. These discussions that we've had in the past, whether we agree or whether we came up with a new question, are truly important to getting to the answer. We often have these discussions and we never come up with the question. You all have presented many, many, many questions. So, we're well on our way there.

We have a shared interest and I'm pleased that all the parties with the stake in our path forward have shown a commitment to work in partnership in a way that people across the globe can only dream about. We have members from various delegations from countries visiting us all the time at the Department of Homeland Security. The one thing that they all want to understand and know about is public-private partnership. They just can't figure out how we're able to do what we do. To me, that's one of the fundamental aspects of us being "America".

As you know, our adversaries in cyberspace from activists to criminals to nation-states exploit our fundamental asymmetry. It's an asymmetry in our network infrastructure, in our training, in our connectivity, and the fact is while all of our systems and networks are globally connected, our defense capabilities are not. And it's not as simple as having a technology solution. We've all realized that at this point. Many of our businesses and citizens at large are blind to the exploits used against them, and worse, uninformed about the opportunities to protect themselves. I am a huge proponent of allowing people to protect themselves and make their own decisions.

Legislation to enhance opportunities for cybersecurity is pending, and fundamental structures to bring more players into this game are absent. . .until now. We know that our efforts need to be multi-tiered, but by sharing cyber threat indicators in near real-time, we reduce the ultimate failure that comes from not being able to communicate. Ultimately, we eliminate the asymmetry of allowing cyber criminals to reap rewards from their efforts, currently. The standing up of this new cyber information sharing and analysis organization is a key step to making cyber exploitation just a little harder for our adversaries. I've asked people, I've had people ask me, "Why is that? Why is this so important?" Because fundamentally, it creates the opportunity for communities of interest to come together and protect themselves. As I travel across the country, there are actually people who think that the government is coming to protect them personally. And I inform them that our responsibility is to help you stand up so that you can protect yourself.

I know the clear observables are down the road. It is yet to be seen how the data will flow, how people will communicate, how ISAOs will stand up, how ISAOs will be terminated. One of the questions that has come up is, "What if we have ISAOs carrying on nefarious activities?" That is a part of the work that you'll do. To help us understand how to get past that. Clearly, the Administration's 2015 legislative proposals aim to increase the speed, quality, and frequency of indicator sharing between the government, the private sector to private sector to private sector. As Miss Spaulding said, the NCCIC was designated as a single federal government portal. A place where the private sector can receive targeted liability protection, a place where the private sector companies receive targeted liability protection for sharing cyber threat indicators. That's <u>if</u> we're able to move forward with legislation that the White House put forward at the beginning of the year.

However, as we have said on many occasions, our key, initially, is not that new ISAOs share with the government, but that they share with whomever they feel assured will help them gain the awareness to protect themselves. EO 13691 lays out a framework for information sharing within the private sector and between private companies and the government by encouraging the development of ISAOs. ISAOs will very nicely complement other activities at DHS and across the government. When we share indicators of compromise in a true automated fashion, we can dream big dreams.

The NCCIC was chosen by the Administration as the single government portal for sharing cyber threat indicators because it's where representatives from the private sector and the government work side-by-side with no agenda other than sharing information and making networks in our public and private infrastructure safer. I can assure you that the NCCIC is working together with the private sector and other government agencies to develop policies for maximizing the near real-time dissemination of all relevant and actionable cyber threat indicators in a way consistent to our fundamental values of privacy, civil liberties, and civil rights. Establishing the NCCIC is the entry way for cyber threat indicators for the private sector to assure uniform application of these important privacy protections. There's a host of programs which are part of a broader system to maximize the near real-time dissemination of information. As we move forward, there will continuously be cyber challenges for us, our stakeholders, the mature companies, the less mature companies. However, the establishment of ISAOs will spring forth from your work to establish voluntary standards and it is a key to our national cyber hygiene.

Going forward, we're building a foundation for integrated situational awareness and coordinated operations across our three key areas of focus: reducing cyber and human risks to our institutions, our local communities, and our people. Not just sector-based: communities of interest.

I was actually asked a question in the last couple of weeks “Has this effort died off? Is there as much interest in this information sharing as there was at the beginning of the year?” I clearly told them, “I don’t know who you are getting your information from, but as I’ve trekked across the country this year, I’ve never seen so much interest in cybersecurity.” The question that people are asking me is “How? How do I get involved?” and the second question they are asking me is “Why didn’t I know about this before?” So, we’re going to keep harping and we’re going to keep working to create a posture that encourages unified protection of asset systems and networks in the private sector and in the government as we begin to set this foundation for prudent management of our communications to improve our cyber posture.

Our goals should be lofty. I’m looking around the room and we have all the players we need in the room. We can change the game. Once we experience an attack or an exploit, the same one should never be able to be used again, because our collective technology, training, and willingness to share information will assure awareness and protection of citizens across the nation. I truly believe this, and the fact that you are here, I’m thinking that you believe it, too. With that, again, I want to congratulate the LMI, University of Texas at San Antonio, and R-CISC team, because they are going to do brilliant work. Thank you.

[Applause.]