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.

Opening Remarks

HEIDI GRAHAM: Welcome to the Information Sharing and Analysis Organization Standards Organization Public Meeting. My name is Heidi Graham and I'll be moderating today's proceedings. Before we move to the first speaker, I would like to go over a few administrative remarks.

First of all, and most importantly, when you need to access the Wi-Fi, you need to find the Guest Net when you're seeking for a connection. Once you get to the guest net, you put in "ISAO3". It doesn't matter whether you have upper or lower case. And then, most importantly, on the back of your name tag is your password. You need to put a zero in front of that password. The zero got dropped off when we printed the name tags. Once you get in there, you'll need to go to an external website, just like you're in a hotel accessing their Wi-Fi. The terms and conditions will come up and then you'll be able to click through and get to your guest access. If you have any questions, don't hesitate to ask and we will help you out.

So, as you all checked in you found the information desk. It will be open until 5:00 this afternoon. If you have not checked in to get your packet and your name tag, please go to the information desk to do so. We will be providing both breakfast and lunch, today, as well as coffee, tea, and water all day. I would like to thank our sponsor Fire Eye for providing us breakfast. We will also be breaking at 11:20, and lunch will be provided and we will have some regularly scheduled twenty-minute breaks which should give you enough time to network or take a phone call or whatever you need to do. We would ask you to wear your badges at all times, and as I mentioned on the back of the badges that all-important password. But also on the back is a letter: A, B, or C. That indicates which small group you'll be joining. We'll share more about that when we get ready to go into the small groups. But you'll be staying with that group during all of the breakout sessions. The restrooms are located out this door and out the south door in the northwest quadrant of this floor down one of the corridors. The men's and women's restrooms are right next to each other, so, it should be right to my left.

I'd like to let you know that LMI is a smoke-free building completely, both the balconies as well as the parking lot and the parking garage. If you need to smoke, please proceed twenty-five yards outside of the building, and you're welcome to smoke. Finally, the walking path that is right outside our beautiful glass windows is not LMI property and we would ask you to please refrain from walking on that walking path. The balconies will be open around 9:00 and we encourage you to take advantage of the nice day before the rain starts. Finally, in terms of emergency procedures, this is the main entrance. If you would out into the main entrance where the security desk of the building is, and proceed across the driveway, to the open area, the grassy area that is out there, that will be our emergency gathering area, should we need to.

Before I introduce our first guest I would like to go over some ground rules for today. They are relatively standard; however, what we'd like to let you all know is that we are providing ample opportunity for you to provide input to us. There will be seven hours of participant input during the small groups. We also have question and comment cards outside of each conference room. Please, feel free if you have a question or a comment that you would like to share (and you don't have an opportunity to share it with the large group) please feel free to write your question or your comment on your card. If you provide your name and your organization, we'll make sure and get back to you. We will also provide minutes via e-mail as well as the participants list at the end of the proceedings. This session, the plenary sessions, are recorded. As you're given the mic, please state your name and your organization so we can capture it. We'd like you to take advantage of all the great opportunities to network and to provide your input today. So, we're going to start promptly on time at the end of each break and at the end of lunch. And as I mentioned before, your breakout group is on the back of your name tag.

Finally, in terms of some common courtesy, if you would not mind please, muting your cell phones. In our conference center there is more than enough space for you to take a phone call should you need to on the balconies and in one of the not-used conference rooms on this floor. And there are charging stations located in the back of this conference room north, as well as the conference room south, and right outside across from the information desk.

And finally, as I get ready to introduce our first speaker, I'd ask you to provide an atmosphere where constructive ideas are developed for today and that you participate as fully as you can during this very important dialogue. Thank you.

Welcome

HEIDI GRAHAM: So, it is without further ado, and my pleasure and honor to introduce Mr. Nelson Ford, LMI's President and CEO. Mr. Ford has spent his career tackling and solving the toughest problems both in private industry and in the federal government and now, by leading LMI in its mission to solve the government's most complex management issues. Ladies and gentlemen, the Honorable Nelson Ford.

[Applause.]

NELSON FORD: Good morning. It's nice to have you all here this morning. Welcome to the first public meeting of the newly established Information Sharing and Analysis Organization Standards Organization and welcome to LMI. I'd especially like to welcome our partner and lead on this project, The University of Texas San Antonio. We've had a long partnership with UTSA and we're pleased to have them. And also, the Retail Cyber Intelligence Sharing Center; our other partner. I'd like to recognize Under Secretary Spaulding from DHS, and Mike Echols from DHS who are with us here this morning.

For those of you who are unfamiliar with LMI, we are a mission-oriented consulting firm dedicated to improving the management of government. We've been in this building for about a year, and we're pleased to be here discussing critical national security interests among the top thinkers in cybersecurity.

I want to tell you a little bit about where LMI came from. We were founded 55 years ago to support the critical needs of the Pentagon for independent, experienced, expert business management professionals, particularly in logistics. LMI was founded to do just this kind of work. Like our partner UTSA, our independence and expertise will help lead this standards organization forward to achieve meaningful results. It is no simple task bringing together government and industry in a public, open-ended, consensus-driven process to agree on a common, voluntary set of standards. That's a tall task.

As you know, there's much at stake here; not only national and economic security, but also personal privacy and protection of confidential information. These are issues that concern citizens, business owners, and public servants; almost everybody. And these are all issues that, if unresolved, will result in a weakened national security posture.

The process is important, and it can be successful. We've proven that. Since 1985, we've been a member of the American National Standards Institute's Accredited Standards Committee that develops standard electronic data interchange messages used to conduct private and public sector business working to build consensus-based data standards. We've brokered more than 1,000 changes through the ANSI-accredited consensus-based governance process. We've represented our clients' interests on standards bodies at the United Nations, OASIS, the Open Travel Alliance and others. Coupled with our partners, UTSA and R-CISC, our experience and prowess in developing consensus-based standards is why we are pleased to be able to assist in the formation of the ISAO.

Success requires cooperation and collaboration between industry, government, and the best minds in academia. Going into today's discussions, I hope you will focus on our common goal, listen to your peers, and accommodate different interests. Let's not let the perfect be the enemy of the good.

I sincerely thank you for joining us this morning and thank you for your civic mindedness. Your participation in today's public meeting brings us one step closer to a state of improved cybersecurity and is vital to protect our national interests. Thank you for being here.

[Applause.]

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.]

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 if 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.]

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 all 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.]

Perspectives from the Front Line

HEIDI GRAHAM: Our next speaker is Mr. Brian Engle. He is the Executive Director of the Retail Cyber Intelligence Sharing Center. Prior to his service as Executive Director, Mr. Engle has served in information security roles in the past for the state of Texas and in the private sector. Ladies and gentlemen, please welcome Mr. Brian Engle.

[Applause.]

BRIAN ENGLE: Thank you. Good morning. I did not get to preface the "brief" part, but she's bright, she's sharp, and she picks up on that and I'm glad that she kept that very brief. As was mentioned, I am the Executive Director of the Retail Cyber Intelligence Sharing Center, or R-CISC, and that is a pretty newly formed ISAC. It positions us with a degree of perspective, but today I wanted to just sort of share and reemphasize why the perspectives of each of you are so important by just giving a few examples of the perspective that the R-CISC and myself bring to bear on this project.

Very briefly, the R-CISC was formed in April of 2014 through incorporation, but became operationally capable, essentially, in February of this year. In that time frame, we've grown pretty rapidly, but what we're seeing is that our growth is in a space that is not as defined as critical infrastructure sectors might wish that to have. So in that, we have a bit of a perspective on how an ecosystem and a business-oriented approach to information sharing create some of these nuances that I think will be very, very important to consider when we start to consider what ISAOs can do.

But at the same time, when we think of retail as a sub-sector component of a critical infrastructure sector, it's critical. It's critical to our lifestyle, it's critical to our economic viability and structure across the Nation and the world. Beyond that, most of my perspective then comes from being a CISO more than trying to head up an information sharing organization.

In that, one of the things I've come to realize is that information sharing is more important across so many different levels than intelligence and tactical intel. Its formative need is really well rendered in what we're doing even with the forming of a ISAO standards organization. The input at the beginning, the ability to come together and share information at the start of something is so critical and it's one of the types of things that many organizations are faced with is how to share information in the forming stages rather than in an evolving state. This sharing includes strategic decision-type things as well as tactical indications of attack and otherwise. So, that bias that I have comes from not just being part of an ISAC but also coming from the place where, as a CISO, there are many questions that you need answered along the way of the formation of a security program.

My passion, much like Mike Echols', is that I think that this is critical. The ability for us to be able to share information to enable security programs to be capable of protecting themselves is just absolutely critical and essential. And the types of things that are needed are the areas of benchmarking, the types of things that are needed to get programs evolved and to mature and to get to the place where the force multiplication factors that enable us to protect at a rapid rate are essential.

Speaking of essential. . . . So, one of the things that I think has become sort of a mindset of many organizations is that they will build information sharing in once they are capable. So they'll develop and get to the place that they will have a story to tell and information to share rather than building it in at the beginning. I would compare this to the sort of age-old principle of, "You build something and then you secure it at the tail end". I think it needs to be flipped around and absolutely has to include information sharing at the onset and the concepts of how to share that information at the building stages. So, the fundamental and essential steps should not be an evolution or a maturity or the type of thing that occurs over time. If you think of a sort of Maslow's Hierarchy of Needs, where you would reach a capable state and then be in a give-back and sharing state. We need to pull that down into the fundamental and essential level of building programs. If you think of that, and you think of the types of organizations that are out there, at all varying degrees of maturity at their start. How do you get information sharing into a capable state at the beginning? And that's going to be our challenge. That's where these perspectives, I think, are so important to be able to look at the history of how some of the ISACs were formed and how they got to the place where they were able to share at the rate that they are now, means that we have to be able to give that capability to organizations that may not be able to deal with tactical intel on Day One. That means helping to build their capabilities at the onset. These standards need to be inclusive of organizations of many different types, many different sizes, many different levels of maturity. We would like to see them grow through capabilities. We want those to be a stair-step approach—that organizations entering at the onset are building towards that very highly tactical and capable level.

We know that the hurdles are significant and many of these obstacles are based upon the types of things where we've seen sharing struggles occur in the past. So we have a rare opportunity to really break down some of those obstacles and do so in a short period of time and make this an effort that is capable of supporting organizations today. I think that's important because sharing is occurring and it's occurring all over the place and there are many organizations that are building and trying to get capable. So, our ability to bring in standards that help develop that capability to the end goal is just super important.

One of the things that I think that we have to be cognizant of is that we cannot just simply hand the tools that we've used for the places that we're at (or that we've gotten to) carte blanche. We just can't give the toolbox to an organization that is trying to develop. We have to enable them to get to that place of being able to use the various different tools that we have in place.

One of the things that we find is the aspect of actionable intelligence. Building a capability of being able to do something means resources. It means applying skills and a lot of those skills are in short supply and high demand. So, we have to consider how to enable those types of sharing capabilities into organizations that are going to have varying opinions on what they consider to be actionable.

The story of context is one of the greatest things that we have to try to do in the building of sharing of intelligence. The quality of intelligence is really highly subjective based upon your capabilities, and a highly capable organization is always going to be able to look at even raw data and say 'I can do something with this'. An organization that has a lot less capability needs to have a lot more of that story built around it before it is handed over. Those are some of the struggles we've seen with information sharing.

So we have to think about not just standards of how the organizations will look at varying different tiers, but I think we have a really good opportunity to assemble the types of things to help rapidly enable capability. And those are some of the things that the R-CISC is trying to do internally, and we've become a very good laboratory for the types of things that these standards organization will develop over time. So, we realize that there aren't magic wands and that these things don't happen overnight. And while we're trying to move at a rapid pace, it means that we're really going to have to leverage things that have worked in the past, and perhaps take that same set of tools and modify them or where we need to create new ones, do so. And those types of templates and things are going to be extremely important.

One of the things that I think I've learned is (or I'll say "observed"): we consider the concept of "lessons learned" and oftentimes we don't truly learn those lessons—we just observe. The things that we observe are just as important to share because those are the types of things that will avoid pitfalls for others. When we look at a lesson that we learn, I think that we have some of those to share and we have others that are just too new (in the sense of, "We haven't gotten to the bottom of what those lessons will be.") The key, again, I see as we look across all of the varying types of organizations that are contributing at the onset and will continue throughout this project are just going to be super critical.

So I'm just going to summarize, briefly, to say that if we can step outside of our goldfish bowl and look at things a little bit differently, and look at the outcome that we're trying to achieve, we can start with certain perspectives and if we consider that those perspectives can be shaped, developed, and evolved to meet the needs of the sharing organizations that are coming to play today and that will come along the way throughout this new world of sharing. It's just going to be critical for us to work together and to cultivate those sharing standards. I told Rick I'd make up the time here. I want to thank each of you for your efforts getting us to this place, because many of you have been, basically, in the front line a lot longer than many of the rest of us. We look to you, we look to your experience, and we thank you for your contribution and look forward to working with you going forward. Back on schedule, sir.

[Applause.]

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 positons 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 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 Sjelin 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.