U.S. Department of Homeland Security
Information Sharing and Analysis Organizations Public Meeting

9:30 to 11:30 a.m.
Wednesday, March 18, 2015

Navy League of the United States
2300 Wilson Boulevard
Arlington, Virginia

Opening Remarks

MIKE ECHOLS: Good morning. My name is Mike Echols. I am Director of the Joint Program Management Office at Department of Homeland Security, Cybersecurity and Communications. We are here this morning to discuss Executive Order 13691, what it is, the implementation of it, and allow the general public to ask questions, find some answers. Again, this is our public meeting, and I say that because we've had a meeting previously. That meeting was with existing ISACs, Information Sharing and Analysis Centers, government coordinating councils, sector coordinating councils, and ISAOs, Information Sharing and Analysis Organizations.

As a public meeting, we are recording and transcribing this meeting. Therefore, if you do not want to be recorded, then you can choose not to say anything. If you speak, you will be recorded.

All right. So just by way of background. Executive Order 13691 came out February 13th, 2015. The President signed this Executive Order out at Stanford University at a Cybersecurity Forum there. The goal of this Executive Order to create an opportunity and enable an opportunity for organizations in the private sector to form information sharing and analysis organizations.

You all may know about ISACs, Information Sharing and Analysis Centers. ISACs are a construct that were created in 1998. They are very sector-based. It is where the private sector can come together, share information, perform analysis, and respond to incidents.

This ISAO Executive Order intends to provide an opportunity for those groups that don't fit neatly into sectors to come together to perform analysis and to share information. That information can be shared with the government, but our focus is not necessarily to stand up organizations that will share information with the government.

The Executive Order is designed to promote information sharing amongst private sector, cybersecurity threat information sharing. We would hope that those organizations that stand up would want to share information with the government, and that is incumbent on us to make sure that the value of the information we provide is such that they would want to. However, just the nature of information sharing, it is a great mitigator, and with the increase and uptick

of cybersecurity attacks, cybersecurity issues, it is important that we mature the cyber education and we build new sets of team members. This Executive Order provides that vehicle for us to do that.

So, today, we have a couple of panels. The individuals that you will hear from are people who work in this field. We work with them regulatory, and they will provide some insights about their experiences. They will provide some insights about what information sharing means, some of the challenges, and some ideas and information on what this Executive Order means in their opinion.

This is a public meeting, so we invite you at the proper time to speak. We don't care if it's anti Executive Order, pro Executive Order. We would like you to just tell us how you feel. We are in the process if gathering information, so that we can meet the requirements of the Executive Order. There are two or three provisions in there that are very important. One, the Secretary of Homeland Security is supposed to promote the formation of ISAOs. Two, DHS is supposed to stand up a standards organization. That organization will work with the private sector, academia, and with government partners to assure that there is a mechanism, a standard for how to stand up ISAOs, how they should operate, and if we look at an organization and we say that's an ISAO, everybody understands what we're talking about. That currently does not exist. There are regional organizations. There are other information sharing organizations that are considered ISAOs because it is an umbrella term; however, there is no standard for what constitutes an ISAO in this context.

We expect that you will see on grants.gov an opportunity to become that standards organization sometime in the spring. Sometime in the fall, we expect that standards organization to be up and running.

Additionally, this Executive Order calls for some changes to the National Industrial Security program. It allows DHS a seat at the table, so that we can have more input into clearances, facility clearances, and how those operations are provided.

Any questions on that? Yes, sir.

SCOTT ALGEIER: Thank you. Scott Algeier with the IT-ISAC. You just made a statement to the effect of the standards are voluntary, but we want to create standards so everybody knows what an ISAO is. So does that mean that an organization that is formed and shares information but chooses for whatever reason to not adopt these standards, does that mean that they will not be recognized by the government as an ISAO?

MIKE ECHOLS: No. I didn't make that statement. The standards organization will work with the government, private sector, to come up with voluntary standards. A determination, the one that you just stated, has not been made.

SCOTT ALGEIER: Okay. I guess I'm a little confused, but that's okay.

MIKE ECHOLS: They will be self-certifying.

SCOTT ALGEIER: So if an organization self-certifies that they meet these standards, they will be recognized by DHS or by the government, but if they don't self-certify, then they will not be considered an ISAO?

MIKE ECHOLS: DHS can go into agreement with an ISAO. At the point of going into agreement, whatever reviews that would normally be done would still be done. If an organization is considered an ISAO, it will tell DHS that it has met certain standards.

SCOTT ALGEIER: So you're saying an organization is considered. By whom? By that organization, or by someone else? I guess my question is, can someone form an organization and call themselves and ISAO and say, "We're sharing information within our membership, but we're not adopting these standards"—will they be considered an ISAO in the view of the government, or would they have to certify that they adopt these standards in order to be considered an ISAO?

MIKE ECHOLS: Our expectation is that the groups that we are sharing with will meet the requirements for being an ISAO.

SCOTT ALGEIER: Okay. So they're voluntary, but you don't get any information from the government if you don't certify that you're meeting those requirements. I just want to make sure.

MIKE ECHOLS: Can you state your question again?

SCOTT ALGEIER: Sure. I just want to make sure I understand, that they're voluntary, these standards are voluntary, but if you don't self-certify that you meet the standards, then you are not going to be receiving information from the government.

MIKE ECHOLS: That's not necessarily true. The government puts out information every day. We have websites. We have—

SCOTT ALGEIER: That's true, but you cannot—

MIKE ECHOLS: Okay. So let's not derail this meeting.

SCOTT ALGEIER: No, I'm not trying to derail.

MIKE ECHOLS: You will probably receive that information—

SCOTT ALGEIER: You asked—

MIKE ECHOLS: —from the panels that are here, and over the course of the next 4 months, we are going to have various workshops to determine the best practices that facilitate that.

SCOTT ALGEIER: Sure. So I'm not trying to derail the meeting. You talked about the voluntary nature, and you talked about the sharing from the government signing CRADA agreements. So I was just wondering if you can be an ISAO and establish yourself as an information sharing vehicle and not meet the standards, and it appears that the answer is yes, you can do that, but it also appears that the answer is—

MIKE ECHOLS: So I didn't mention CRADA agreements? You have a little more information than most people in the room, and at this one moment, I don't want to confuse them. The CRADA agreement is potentially a vehicle that we would use to make agreement, not necessarily a fact.

There are a lot of facts that have not been determined yet. They will be determined through public meetings, through workshops, through what we hear from the public, and as a matter of fact, anyone who wishes to make a comment can send that comment to isao@hq.dhs.gov.

SCOTT ALGEIER: All right. Thank you, Mike. I appreciate it.

MIKE ECHOLS: Thanks. Sir?

DAN BART: Dan Bart, Valley View Corporation. You mentioned the bid for the SO would be in spring with the expectation that it will be stood up by fall. In the open competitive bidding process, I thought I heard mention at the last meeting that it may be a two-step process with kind of an RFI initially followed by an RFP, or is it going to be a one-shot kind of a thing?

MIKE ECHOLS: The grants process works slightly different. On the website for the Office of Chief Financial Officer, you can find the process. We will follow that process.

And we will have more opportunities for questions at a later time, but I want to bring the panel up. I'm glad that we've got this meeting off and running. I don't like a quiet meeting. So I want to bring up Mr. Mike Darling. Mike is a senior official at Cybersecurity and Communications, and he is going to lead this panel.

Panel: ISAO Challenges and Opportunities Dialogue

MIKE DARLING: All right. If I could get the panelists to take their seats up front, that would be great. Let me just get myself organized here.

I am actually very excited about this. This is something that I think is really important. I want to thank our panelists for taking the time out of their day to share their thoughts and insights with us.

As Mike said, there are a lot of questions that are unanswered at this point, and what we very much care about at the Department of Homeland Security is that we have that full conversation. This initiative is the administration listening to the private sector and saying the government needs to do more to help with information sharing. This is one of the things that we're trying to do to get there.

Kind of the theory of the case behind it is that—I think we all know that cybersecurity is a team sport, and the government is at the center of this universe. So we very much need to figure out how we can help catalyze more information sharing. As Mike said earlier, if this catalyzing an ISAO being formed with the private sector who never wants to talk to the government, that's a win from our perspective. We obviously want to work collaboratively and that sort of thing with the private sector, but what we really care about is helping to move the ball forward on the information sharing, and that builds on a lot of the good work that the ISACs have done. We've got a lot of lessons learned, and trying to figure out how to make more of that, more of those good things happen out there is something that we very much care about.

With that said, what I am going to do is just kind of kick it off. We'll start off with a couple questions that I'll have for the panelists, and then we'll open it up briefly at the end for questions. One of the challenges, I think, always with these sorts of things is keeping on time. I will do my best to keep us on time, but I think the full and open conversation is important.

With that, I'd ask each of our panelists just to introduce themselves and describe their unique requirements for their organizations in the developments of standards that they may have, their fears, the opportunities they see. I would ask each of the panelists to keep it to about 4 or 5 minutes apiece, so that we can move on to the other questions as well.

Scott, if you don't mind kicking it off?

SCOTT ALGEIER: Sure. That's fine. Thank you. Good morning. My name is Scott Algeier. I am the Executive Director of the Information Technology ISAC. I want to thank Mike and the team for giving me the opportunity to be on the panel today and also thank Mike for the opportunity to express my questions previously. It's questions that are out there in the community, what does it mean to adopt the standards or what happens if you decide, if you choose not to adopt, who determines whether you've adopted them. Similar questions we have when the NIST cybersecurity framework was developed: what does it mean to use, what does it mean to adopt, what does it meant to implement, what's the right wording. So I appreciate the opportunity to get those concerns out there in the beginning and appreciate Mike's candid responses.

For the IT-ISAC, we were formed in 2000. As a result of the request made through PDD 63, we were one of the first industries to organize, to self-organize an ISAC. We have been operational since 2001, so it took us—after you incorporate, you need to sign the member agreement to get the members, get money in, do a contract with a vendor to do your services, so it takes a little bit of time. We became operational in 2001.

We have been doing this for quite some time. We have tried different models of doing it within our membership, and we have developed a model that is unique to our sector that represents our sector interests, that represents the competitive interest within our membership. For example, we obviously have companies who provide threat intelligence services, and we need to find a way to provide value to our members without competing with those companies.

We have banks. All the banks are competing for mortgages, and they all want your money in their bank account, but they are not competing in the security market space, like a lot of my member companies are. So we have developed a unique structure that enables us to facilitate information sharing through communities, specialized communities of interest, and get subject-matter experts who are working on the same business topics, same security areas, talking with other subject-matter experts from some of the world's leading technology companies.

We are international. We have memberships from companies who are not based in the United States, and obviously, our members provide products and services outside of the United States. So doing the international exchange, international information sharing is an important concern for us.

Obviously, we're member driven. Our primary responsibility is to meet the needs of our members. If we don't do that, they won't renew their membership. If we don't meet their needs, they won't be referring their colleagues to join the organization, and we have been very successful in being a member-driven organization that has the flexibility to meet the changing needs of our members, as the threat changes, as the technology changes, as the sector changes.

So I'll wrap up here with the four main themes that I think you are going to hear me talk about today on the panel, and one is that ISACs have the experience and history. There's many ISACs out there. We have the experience in information sharing. We have a proven history of doing information, and I think some of the key learnings from the ISAC experiences should be the cornerstones for creating this ISAO construct.

Information sharing standards and best practices should be industry driven and not prescriptive and not overly burdensome. You can't tell us how to do things because each member organization has unique needs, so we can't have a one-size-fits-all solution.

The ISAO construct should be—we need to consider the global nature of the threat and information challenges. The cyber threat isn't based on a region. It's not based on a country. It's a global threat, and the construct needs to consider this.

And then the final theme that you will be hearing me talk a lot about in this meeting and other upcoming meetings is that information sharing is a tool. The goal is to create situation awareness, and we need to keep that in mind as we talk about information sharing, information sharing, and information sharing, what's the strategy for creating a capability to turn this

information into a national situational awareness, and then also how we can share this situation awareness with our international partners. So thank you very much.

MIKE DARLING: Thank you, Scott. Tanner.

TANNER DOUCET: Thanks. I agree with Scott, and thank you, Mike Echols for organizing this. Our President and CEO, Larry Clinton, he regrets he couldn't make it this morning, but I am Tanner Doucet, and I am the Director of Policy at the Internet Security Alliance.

Quickly, for those that don't know, ISA is a multi-sector trade association, and we focus exclusively on cybersecurity. Our mission is to integrate advanced technology with economics and public policy and create a sustainable system for cybersecurity. So ISA is not an ISAC. We originally started as an ISAC back in 2000, but that's no longer one of our main functions.

From the outset, I want to be clear that any re-architecture of our information sharing system through the ISAO process needs to be based on the successful functions being provided by the current system, and that includes the ISACs. ISA's prime directive for this is do no harm. So we can't afford to create more regulatory systems, and we can't afford to muddy our cybersecurity efforts with competing issues and missions.

ISA's goal for this effort is to work with the stewards of our current system and our government partners and achieve four major goals, and we need to make our information sharing system easier, less costly, more accessible, and the information being shared needs to be as actionable as we can.

We anticipate that this will require leveraging the ISACs and further enabling them as well as the vast information sharing system that currently exists. As we launch this review process, ISA proposes three initial areas for consideration. One, we need to review the sector model for information sharing. For example, the ISA board chair is the CIO from GE, and what sector does GE fit in? In truth, probably about 11 sectors, and currently, they participate in a lot of ISACs. GE isn't really alone. Many of our major financial institutions and event sector members, they create their own uniquely tailored software and hardware, so they belong in financial services, IT, and others.

The multi-sector as well as international nature of modern business may not fit well with the historic sector-by-sector model. So rather than using the historic sector labels as our organizing principle for information sharing, we could be more effective by grouping these companies based on economies of scope and scale. They have more in common and, hence, would make sharing easier.

The second area that we think needs to be considered moving forward is how do we get more small players involved, and this has been sort of a challenge in the past, mainly due to barriers of cost, time, and insufficient resources, both financial and more in the technical realm, and small companies, which has sort of inhibited some of the participation there. The truth is that

every small company wants the same thing, and that's really to become a large company. So any extra resources that they have is likely to go to sales and marketing rather than security, so we need to find ways of incentivizing these groups to participate. ISA has a detailed proposal in this regard, and perhaps ours isn't the best model, but one thing is clear, I think we need to sort of incorporate more small to medium businesses in this organization.

The third major area we would like to review is international. Cyber attacks nowadays are international issues, and the notion that we have a U.S.-only solution, I think is sort of outdated. I think, obviously, there are some legal issues and some trust issues here, but I think that is sort of the point, that we need to start to discuss these issues and get them on the table.

ISA sees the ISAO initiative to identify the best practices as an opportunity to move toward these goals, and we're anxious to engage with partners, both in the private and in the public sectors.

MIKE DARLING: Thank you, Tanner. Chris?

CHRIS FOLK: Good morning. Thanks, Mike. This is an exciting time and kind of a wonderful way to engage in this important topic in a public forum like this. My name is Chris Folk. I'm privileged to have spent the better part of my career at the MITRE Corporation, working the expansive Homeland Security sets of issues. MITRE is a not-for-profit. We operate federally funded research and development centers that are chartered to work in the public interest. In that role, we are kind of vendor, product, and solution agnostic. Instead, what we're trying to do is make sure that the needs of the public are well represented.

So since the President's Commission on infrastructure protection back in 1997, MITRE has been actively engaging with the private sector and in this area of information sharing, helping sort of stand up the initial sets of ISACs back in the late 1990s and early 2000s, supporting the FBI NIPC program and then subsequently, as DHS stood up, helping them stand up and enable them.

The focus on standards and vulnerability and then threat intelligence exchanges has also been something that we have been keenly involved in.

Finally, looking at regional and functional-based partnerships, the key message here is that our thinking has continued to evolve over the course of these 20 years as it has in the community. One of the things that MITRE has found over the course of these 20 years is that the exchange of information is, A, not the thing. Scott indicated earlier this is not about information sharing as the end state. It's about an enablement capability.

Interestingly enough, when the ISACs were formed, the focus was on sharing compromise and vulnerability information. That was what we knew. That's what we had. That's what the challenge was at the time, and it turns out that, unfortunately, that's the hardest thing to share. People, ironically, are less likely to share that k individual of information, and unfortunately, also, it's probably the least valuable information that can be shared.

Sharing threat intelligence and its predecessor, vulnerability information, has always been a way to unite the cyber defenders along a common set of ideas. That compromise of information has allowed those defenders to come together in ways that they never would have thought to do before that crosses those industry boundaries.

When the White House came out with the Executive Order and charged that organizations engage in sharing of information related to cybersecurity risk and incidents play an invaluable role in the collective cybersecurity in the United States, we couldn't agree more. I think that this is about enabling those defenders, wherever they sit, to bring forward the best of breed and help inform and strengthen that ecosystem.

To that end, MITRE has led the way in developing, participating, and enabling a wide range of information-sharing capabilities and their underlying structures. As a partner to the U.S. government in enabling areas of research and development, we're under constant pressure from adversaries. So MITRE, like all companies, sits on the Internet. We're an attractive target, and a position as a government contractor means we're not in short supply of threats. It's what we're doing about it, what we're learning from it that has been most valuable to how we think about threats and how we share that information back with others. So we've learned a lot over the last 5 or 6 years about how those threats propagate and what we can do with those.

So we see a range of options, tools, and structures available for today's cyber defenders. Today, cyber defenders don't sit neatly in one-size larger nesting eggs. We're a society of interconnected, interdependent points on a network that itself knows no boundaries. The range of cyber defenders is huge, from a few individuals along common shared views or outcomes to businesses operating across multiple business verticals to regional entities, trade associations, and other groups who bind themselves to others for shared cause and purpose. Sharing vulnerabilities, sharing threat information, best practices, tools, techniques, procedures, all of those are individual value to those defending the economy and national security.

The attacks we see today don't neatly occur along some static national line. Rather, our adaptive adversaries are learning. So they are adapting themselves, and they are sharing amongst themselves. Isn't it time that the defenders figured out that they can share in different constructs and allow that sharing to meet the cyber threat where it is today?

So what we found are some key success factors in these various regional sector, trade association, or organizational dependent sharing models, and they really come down to a couple things. Information sharing in its broadest sense must meet the participants where they are. This is not about dragging everybody to a similar place and insisting that they all look and feel the same way. MITRE has been a part of various information sharing organizations, constructs, over the past 20 years. Some of them work; some of them don't. Some of them continue; some of them have failed. So it's about finding where those constituents are, what matters to them and their business and enabling those things. It must meet the needs of its

members, and not every participant will have the same goal. So this is not about a maturity model that moves us along a particular route that says you are going to go from A to B to C. This is about recognizing that different organizations are going to have different endpoints in getting them there.

So I think there's a lot of different paths that we can take here and a few different models. Hub and spoke versus mesh crowd sourcing, this enables both and allows us to interconnect these sharing groups that exist today. I think that a standards organization will be an enabler to getting information sharing expanded to new entities that find themselves in a need to come together and benefit from the collective wisdom of the crowds, without forcing them in a particular path that doesn't meet their needs. Thank you.

MIKE DARLING: Thank you, Chris. Tim?

TIM ROXEY: Thank you very much. Last time I was here, I said something like embrace your inner regulator, and I kind of sort of mean that. As an international ISAC with membership in Mexico, Canada, and the United States, the NERC ES-ISAC is not a pay-to-play. It is free to all in the electric sector ISAC. We are operated by NERC under Section 215 funding. We have been endorsed by the sector-specific agent, so we have a formal relationship with our sector-specific agent in writing from Department of Energy, supporting the efforts of NERC, supporting the efforts of the ISAC, and we have also been selected as the ISAC for the inner electricity sector by the Electricity Sector Coordinating Council, which is a group of 30 CEOs representing essentially 80 percent of the bulk power system in North America.

We are also, largely enough, a standard development organization. Probably, people have heard about the Critical Infrastructure Protection Standards. That's part of what we do. We also do so-called "Section 693 standards" from FERC. That's reliability of the grid writ large—vegetation management, frequency control, et cetera. So NERC has been in this realm of writing and developing consensus-based ANSI-certified process standards for quite some time. We are certainly not on the first rodeo at either the standards organization, and we are clearly not on a first rodeo with developing and operating an ISAC. We have potentially up to 4,000-some-odd electric utility companies inside North America that could become part of the ES-ISAC.

We also support the Title 10-regulated folks, and for those who would like to know who that is, that's the nuclear sector in the United States and the nuclear sector in Canada, under a different set of regulations. Information sharing with them is also vital. Some of that information that the nuclear sector deals with is required by regulation, just like it is in the United States and just like it is in the electricity sector required by standards. That is a baseline set of required information upon which the ISAC builds surge risk controls, which is the alerts and notification process, the threats and vulnerability indicators of compromise, et cetera, et cetera, et cetera.

We work with many, many nonregulated entities. So entities that are too small to really swing a hard hit against the bulk power system, we support them the same way as we support the largest companies in North America. It is critical that we support all of the electricity sector space in the United States. The unique characteristic of a cyber compromise being horizontally scalable and looking for the weak link may find it in any organization. There is not a single organization that probably has not been compromised at some level already.

We already work with several ISAOs, and as this turns out, we are one. So we're comfortable with the ISAO.

No one has mentioned INPO. I'll just toss that out there as a nonregulated information sharing and analysis organization called the Institute of National Nuclear Power Plant Operators, I believe, and that's an interesting model because inside of a regulated space with the NRC, INPO exists and supports the nuclear utilities within United States extremely well, driving to excellence instead of driving to a baseload of regulation.

And in addition to the information sharing and analysis functions that are normal, classic, threats and indicators of compromise, like Chris indicated, and a variety of other things, we also provide sector outreach, training, and we run the largest grid exercise on the planet at least once every other year. We gather 2,000-plus of our best friends and many, many companies, and we run a very complex hardcore electric grid attack recovery exercise, so that's one of the things that we do.

And we look forward to the future. I think that this establishment of ISAOs and the relationship of some minimalist requirements vis-à-vis standards for the ISAO to be able to facilitate whatever forward-going conversation would take place with DHS, I think that's fine. That's a DHS issue. It will have relatively zero impact on the ES-ISAC because we're already up and running and moving, and we already have the designated endorsement of the specific agency and the Electricity Subsector Coordinating Council designating us, but I would like to request that the standards only apply to the ISAO structure and not cascade down into the membership. So don't pass a standard that reaches down through the organization and impacts the ability of the membership or controls the way the membership of the organization behaves relative to its selected ISAO or ISAC. Thank you.

MIKE DARLING: Thank you, Tim. So a great intro, and I think there's a couple themes coming out of there. As a precursor to a couple follow-along questions, what we hear is that information is not the end. It's the means. And what we're really concerned about is the connection of those defenses. There's a lot of bad guys out there who are coordinating. We can look at that as well. It's a complex world. There's a lot of different companies out there that we have to figure out something flexible enough to accommodate those worlds.

With that, Chris, in the overall cyber threat landscape, not just your sector—and you cut across a number of sectors—where do you see the greatest need for improved situational awareness? In other words, what gap in the marketplace can these ISAOs help shore up and drive forward?

CHRIS FOLK: Thanks. I think the real challenge has been in recognizing that not everybody is created equal. When the initial information sharing arrangements that the government tried to help get going 5 or 6 years ago weren't meeting the needs of the customers, what we are finding is the information was coming from—the government was taking too long to get to us, that it was finding its way to us through other mechanisms and other venues faster. I think the greatest need is to expedite that. I think that it is about getting these organizations to find how to get their defenses put in place today and not wait for long periods of time.

The adversary is flexible. They are changing their TTPs. We're seeing the adversaries adapting to how we're organized and sharing information today. They recognize that we're aligned along 16 sectors, and so guess what? They're changing how they are attacking us based on that knowledge. So when those kinds of adaptive adversary behaviors happen and you have static defenses that are aligned along a construct where you have a bureaucracy that won't allow you to change as fast as they are, you are not meeting the needs of the constituents.

MIKE DARLING: Okay. Great. So, with that in mind, Tim, Chris talked a little bit about meeting the needs of the constituents. That being said, what do you think it would take for your group to integrate and share with the ISAOs that do spring up as in meeting some of the needs of these constituents, or how would you make sure of data coming out of the government partners, like NCCIC?

TIM ROXEY: Well, number one, we already do share with ISAOs. Like I said, there are several ISAOs in the electric space right now who represent their membership very well, who are very small, who are very focused. For instance, certain particular kinds of verticals within the electricity space, whatever those may be, have organized themselves in small collections, and their SOC, security operations center, and my SOC, they talk virtually daily. A little differentiator is that the ES-ISAC along with the more formal ISACs have a relationship with, as Paul Stockton would say, the left- and right-hand side of boom. So when you move to the right-hand side of boom and there is a large-scale impact to whatever your sector may be or whatever your ISAO maybe, but in particular, the ISACs, you have a formal relationship with the unified coordination group, within Homeland Security. There is a certain structure up around how that information flows from the sector to fusion at the NCCIC, and there's a certain structure defined within the USG documentation that talks about how that information flows back out to the sector, in my case, the electric sector.

We have seats at the NCCIC. We understand those people very well. There is an Energizer Program at the NCCIC, and if you don't know what that is, talk to some of the people in the community, and they will help you understand that. But we have taken in our sector, that Energizer Program and made what we call "energizer light," because it's a non-classified document in our world, and that non-classified in our world is how you create your crisis response plans for a company or for a collection, and that's the way that our Electricity Subsector Coordinating Council works with the ES-ISAC, works with the NCCIC. So we put all of that together in writing, in documents first, and then you exercise that several times, very, very

strategic-level exercises with your CEOs, and then down to exercising it with your various SOCs, NOCs, and the ISAC. That is going to happen again here in another—my friend Bill Lawrence would absolutely know right off the top of his had how many days, but it's 200-some-odd days—when we do GridEx III, which will be again 2,000-some-odd people, many, many hundreds of companies and all across North America. We feel that we are doing very well in that regard, and we look forward to finding those ISAOs that can bring value to our information sharing partnerships.

MIKE DARLING: It sounds like a lot of what you talked about is the information and the actionable information. There is another theme. So I want to keep with that theme here for a second. Tanner, it's been mentioned here today, and one of the critiques that we get from our current information sharing efforts is that the information that flows isn't always actionable, not necessarily as useful as it could be, if what we're really talking about is connecting the defenses.

If you were talking to the ISAO standards organization today, how would you recommend that they define actionable information? What qualifies should a piece of threat information possess to qualify as truly useful for enabling one's network to invest?

TANNER DOUCET: I think in terms of getting some of this stuff out on the table, one thing is making sure that the information is as timely and actionable as possible, and particularly for the small- and medium-sized businesses, one thing, sort of like I said earlier, they need information that's more simplified a lot of times. For the most part, these small guys don't really want to sit on these weekly calls. They want to know what button to push to stop the attacks.

I think one way to get this broader SMB action moving forward would be to kind of simplify some of the information that's being shared. One way to do that, for example, is sort of—a lot of the big guys, the notion of outbound traffic—sorry—defending the network and firewalls is sort of outdated. You have to assume that the adversary has gotten into your system, and once you make that assumption, the game now becomes watching that code and seeing what happens, seeing where it tries to phone home. So if you're able to keep track of where that code phones home and that outbound traffic out to bad IP addresses, that is information that I think can easily be shared down through some of the small- and medium-sized organizations.

MIKE DARLING: Great. As we talk about actionable information and expanding the aperture and looking at organizations that are actually fulfilling their customer requirements, Scott, you're already a member of a successful ISAC with a fairly diverse set of customers. Given the experience that you have and some of the lesson learned—I know you mentioned this earlier—what advice would you give to a group looking to form their own OSAO?

SCOTT ALGEIER: Thank you. My advice is kind of pretty simple, I guess. It is understanding what your customer need is and work with them to find a way to deliver their needs. You need understanding. Your members need to have conversations with each other about what information is valuable to them because not everybody is looking for the same piece of

information. You also have people within member companies who have specific expertise, who are dying to talk to people with other companies in a trusted forum, who have similar expertise, who are facing the same challenges, so that they can compare notes and strategies and identify what's worked in the past.

One quick example, we've had a couple recent—some of it is information sharing, "Here is an indicator of compromise," but others of it is getting people on the phone and saying, "Hey, how do you set up a program to define and advance threats into your network? How do you develop a program within your company to do data, big data analytics, so you can take all those different pieces of data that you have and correlate it and identify which is the most important, "Which of these indicators do I need to go check out first?"

So in terms of best practices in starting an organization, you need to understand what the gap is that your organization is filling and how you are going to meet that gap. It's really that simple, is understanding why you need it and understanding what value you provide to your members.

MIKE DARLING: Okay. Great. Looking at how you provide a value to the members—and I think that's something that really resonates with me personally at DHS, and I know the government, we try and we need to drive more of it and show more value in this space. We have got some good foundations, but like everything else, we want to move this forward and kind of catalyze these defenses.

Chris, is actually helping to drive that value proposition through a broader set of ISAO standards, developing the ISAO standards and best practice models assumes a consensus amongst industry. In your opinion, what might consensus standards look like among industry, especially considering the fairly diverse groups with different goals and requirements?

CHRIS FOLK: I think that is going to be the million-dollar question, so let me give you some experiences that we have seen. Not an advertisement, but some of the various information sharing and analysis organizations that have come about more recently than the ISAC model are sort of these regional approaches. So we're seeing a couple of these around the country, and they're in various forms and fashions of standing up.

The experience that we have had in participating with these organizations, no two sizes are the same. I will say that we are working with groups in Chicago, and we're working with groups in Boston. The Boston group, for instance, was aghast, that they would want any federal participation in their group, because they felt that the 27 companies and organizations that were coming together were best able to really have that trust amongst them, and they wanted to keep the government out, and that was what worked for the member organizations. Chicago is the exact opposite. They had a longstanding great relationship with the FBI, and they said the FBI has to be at the seat at the table, and they have to be part of this.

So what we have found is that there is no one-size-fits-all approach to this. The standards that will have to be developed are going to be about what the outcome is for these organizational—

individual pieces of this organization, not about what works for any one large group.

The message that we have heard over and over and over again is trust. You can't go anywhere without talking about trust. How you build trust, how you scale that building of trust is incredibly challenging. It is really, really hard, and it goes beyond—it goes beyond any kind of single set solution that's out there.

We have had to watch organizations say, "I am going to put more skin in the game than somebody else." We have had to have organizations that were willing to be a little bit further out.

I believe Tanner talked about organizations that are little bit more mature in their thinking. Sometimes those are the big brothers that are sort of the kick-starter to these capabilities. I think you need to look at standards that allow for models that meet the members' needs, and sometimes it's going to be removing those obstacles from them right up front.

For instance, we have organizations in the Cleveland area that we have been watching that are interested in standing up a threat-sharing organization, and their biggest obstacles are establishing a business practice that is self-sustaining for them in the future years. Everyone is willing to come together for the first year, spend $50,000 out of their marketing budget to get these things up and running because it's new, it's novel. It is what is going to keep these guys year 2, 3, 4, and 5, and their challenge is in finding those members that are willing to show up time and time again after the novelty has worn off, and that's something that we have seen over all of these new organizations that are standing up. So it can't be new and novel. It's got to be a self-sustaining business model, and a standards organization can help them set not a standard business model, but can really help them figure out what a business model looks like, what business models are self-sustaining to the members and understanding why the members come on day one and why they show up on day 366 when the new and novel has worn off.

MIKE DARLING: I think great points. Great points. So that business model is something that I think is important, and some of the things people struggle with are the vendor services and that type of thing.

Tim, knowing that many of your customers, many of your member groups utilize the services of businesses like law forms or HVAC service providers and other small businesses, how do you think your ISAC might be able to plug in with these types of ISAOs if they were to form, and how might they help improve your situational awareness, and vice versa?

TIM ROXEY: Well, oddly enough, there's a significant dependency on electricity for these organizations, so huge law firms, collections thereof, HVAC vendors in particular, one of the my favorite groups because nobody remembers to look at the thermostat and attach the thermostat. That certainly wouldn't have been a breach within the last year.

But these organizations, if they form ISAOs, I would look forward to coordinating with them as an ISAC, the same as I would coordinate with any of my member companies, simply because my lawyers talk to their lawyers, and my HVAC service folk talk to their HVAC service folk. And it's not just NERC and the ES-ISAC. It's large facilities have HVAC requirements as well.

Now, there is kind of a restriction, if you will. I won't necessarily let the HVAC or the vendor community directly into the asset owner or operator component of my portal because that's for the asset owner or operators, but that does not mean that the threat indicators and compromises that we see cannot be shared with the other sectors. We do this all the time. This is part of our day job is to talk amongst ourselves, which we do at ten o'clock, starting in 5 minutes, again, today, and we'll do it again tomorrow, and we'll do it again tomorrow, and we will do that 366 days from now. And I am blessed to be in a sector that is already funded. So I have that business model advantage, if you will, in terms of longevity, and I would welcome working with other ISAOs because you could actually see, as we see in some other sectors, compromises of a law firm leading to a compromise of a merger or acquisition overseas, and that could have an impact in terms of the financial resources of somebody. So it's a convoluted web they weave, but nevertheless, that particular compromise may be exactly the same kind of compromise that could happen in the energy space. It's just that the intent was to steal M&A information and not stela energy information.

So if we can support them, they can support us, and we can get a consistent set. As we said, actionable intelligence means you have the intelligence necessary to go in and push a button, take an action, block a punch. If we can get there with the ISAOs, good on us. I think that's our stated endpoint to improve situational awareness horizontally across all sectors.

MIKE DARLING: Right. I would like to pull that string a little bit. So we talk about law firms. You had mentioned HVACs, but the experience of the panel here, I think is important to think about this a little bit more. What other groups are out there?

Scott, as an established ISAC, fairly mature, what groups are out there that you would most like to share information with or receive information that you don't already receive, and why?

SCOTT ALGEIER: Sure. The IT-ISAC, we obviously support information sharing. We have a business model where we bring into our membership, companies from sectors that don't always have an established information sharing mechanism or an ISAC. For example, we have a small but growing number of food and agricultural companies who participate in the IT-ISAC because they have some unique threats. They have some unique business interests, and they need a forum to talk about them. So instead of spending the resources to build something from scratch and taking the time to build something from scratch, they draw on the IT-ISAC. We get them approved for membership, and in a matter of days, they are exchanging information, threat information with each other, and receiving the information that our other members share.

We proposed at multiple times to partner with the Department of Homeland Security where you can go out and reach underserved communities and bring them into the IT-ISAC. Those conversations haven't gotten anywhere where we haven't actually had a formal discussion with the Department about our ideas. We submitted the first idea in April. I think it was 2012, and then last August, so we'd still be happy to have a conversation with the Department on how we can work together to fill the needs of some of these underserved communities, small businesses among them.

So we support the concept of sharing information. We have been doing it. We have been actively engaged in outreach to companies and sectors that are underserved, who don't have their own forum, for many years now, and we look forward to continuing in that effort.

MIKE DARLING: Okay. To kind of close this out—I am just cognizant of the time—I want to give the audience some opportunities to ask the panelists a few questions. Last question for you, Tanner. From your perspective, what does the perfect information sharing community look like?

TANNER DOUCET: Well, I think the perfect information sharing community in the future would sort of leverage all of the things that we have been discussing, getting more folks from the SMB community involved, and I think that will take some incentives to sort of go along those lines. Liability protection will be included in there for the big players, and for the small players, maybe some tax incentives. That's another one.

For the utilities, maybe fast-track permitting, all this kind of stuff, but I think the perfect environment would be where all of these folks, all of these players, from the HVAC folks up to the bigger guys, are all sharing, they're all involved in the same sharing system.

MIKE DARLING: Okay. Great answers and insights up to this point.

[Applause.]

MIKE DARLING: But we still got 10 minutes. We've got these guys for 10 minutes. From the audience, do we have questions for our panelists?

DAN BART: Dan Bart, Valley View Corporation. The Executive Order is focused on cyber sharing of information, but for those who have labored into the critical infrastructure protection vineyards for a long time will remember the discussion of I can have a cyber attack on cyber assets, I can have a cyber attack on physical assets, as Tim knows, I can have physical attacks on cyber assets as well as physical on physical. And in addition to the terrorists and the bad guys, sometimes mother nature is the worst terrorist of all in terms of some of the destructive power she has. Is it a mistake to have ISAOs focusing only on cyber, given the realities of the real world in the four different attack vectors? And from the experience of the two ISACs that are represented on the panel, I'm sure you don't just focus on cyber, but you

focus on all of the things, and aren't you all hazard-type ISACs? Is that a better model that cyber-only ISAOs?

CHRIS FOLK: So to jump on that one right away, back in the early days of writing the NIP, Bob Stephan had the pen, I believe, Colonel Bob Stephan from DHS. We were all about all hazards. We have never walked back from all hazards. When we do our training exercises, they are always blended attacks where one punch happens, and the second punch, you will never see because it is probably going to be an APT so slow and low that you're going to have to really try and figure out what things happened.

The original versions of the NIP, the original version all the way back to 1998, Secretary Richardson's letter to North American Reliability Council, the earlier version of NERC, which actually started the ISAC at that time, never did say all cyber. So we don't do all cyber. You can hurt folk just as easily, physically, probably simpler in some cases, but one of my goals, if you will, aspirational goal is to be so damn good at cyber defenses that I force my cyber adversary to stand in front of me because now I'm into a physical engagement, and that's one I know for decades. That's one of the earliest types of defense we have, which is why we have physical security boundaries and all that other stuff. Those are relatively straightforward and understandable. Cyber sometimes is very arcane, but we do both.

SCOTT ALGEIER: So IT-ISAC, very similar. We take an all-hazards approach. We're part of the—we integrate it into the National Infrastructure Coordinating Centers, critical infrastructure resource, private sector annex, which basically means that we provide me and another analyst to help coordinate response toward physical threats. We're reconstituting a forum for chief security officers, physical security business continuity personnel within our membership, but we do share physical security information with our members regularly.

Obviously, the focus of the EO was on cyber. My own personal view is that I am not going to tell another organization how they need to provide value to their members. If their members want a cyber organization, then their members can have a cyber-only organization. Perhaps they get their physical needs done by someone else, but for the IT-ISAC, we're all hazards.

MIKE DARLING: And I would like to point out at DHS, we remain committed to looking at all hazards, through our partners at the Office of Infrastructure Protection—and the EO actually does have a provision for integrated it in here.

We had some other questions from the other side of the room.

CORY CASANAVE: Thank you, gentlemen. Cory Casanave. I am working on risk and threat information sharing standards at the Object Management Group, and in fact, we're having Individual Day on that Monday in Reston. I hope to see you all there.

There has been a theme of—this is international, global, all hazards, multi-domain—team sport, and as we know, in government-led efforts, there is a tendency to close things off. How do we

make this a federation, a real federation of the information, of the organizations, of the standards so that we can be inclusive of all those different concerns?

CHRIS FOLK: Let me take a shot first at answering that. I believe that—this is in my opinion-that the first time that the government has stepped back and said—and Mike said this at the beginning, and the other Mike said that even before that—this is about empowering these organizations. This is not, well, it's government-led. If you notice, it's not a contract that they're letting. The approach is a grant. So contracts apply that you do something and deliver it on behalf of the government or to the government. This is, in my opinion and as I read this, this is about enabling the enterprise of you guys in this room to be better secured. It is not about making sure that the government has a seat at the table, and so this independent standards organization is going to work with the government to sort of help shape that, but the intent is that this is not a government-led set of solutions.

I think what the value in that is—and I mentioned this earlier—is getting those roadblocks out of the way of these organizations up front because there's a lot of challenges in cyber defense and information sharing, and people put up artificial roadblocks all the time. And some of them are legitimate, and some of them aren't. This organization is trying to say, "Hey, look, here is what's worked. It's not necessarily going to work for you, but let's work with you to help you build something that is workable for you, and it's not about the government benefiting directly. It's about the fact that the ecosystem is stronger, the fact that the network defenses are better, and it allows the government to say, "I don't have to spend $5,000 over here sending an incident response team for $10,000 or whatever it is an hour to remediate something because you guys have taken care of that by joining these information sharing analysis organizations, putting in place cyber defenses, and then actually defeating the adversary before it became an incident.

So I think that it's about removing those roadblocks, and I'm very encouraged by the fact that the government and the administration has recognized that this is not a government problem to solve, that this is about how does the government partner with industry in a completely different way than they have in the area of cyber defense before. It is not about the NCCIC solving your problems. It's about those in this room solving the problems as members of that team.

MIKE DARLING: Absolutely. I think that's a great summation, and I will say I think we are fairly clear that there will be some bumps in the road. It's a hard thing to do, but again, this is about the partnership and building the partnership and getting the—it's a good way to put it, the roadblocks out of the way.

I think we had another question back here.

TOM LAMB: Hi. Tom Lamb from ISACA, IT professional global organization. So my question is kind of twofold. One is, what's going to be done to enable the better communication and

facilitation between the ISAO concept and the ISACs? And I say that from an outside perspective as well as a global perspective.

One of the things, certainly, that we hear from organizations globally is they're a bit confused about the Executive Order and the concepts within that, and so when I heard Scott's comments about the preliminary aspect up front, I think it can be worked out, but I think there needs to probably be some better communication outside.

MIKE DARLING: I think that's an important point to take, and again, as Chris mentioned, we are looking at the different model, and that takes some time for people to kind of get their arms around, so the communication point, I think is key, one of the reasons we're here today.

I think we got time for about one more.

ATTENDEE: Good morning. First of all, this is a terrific panel. Thank you very much, and thank you for the host.

Let me offer maybe a little different point of view and get the reaction from the panel today. I argue that, in many respects here, we're having the wrong conversation. The notion of an Executive Order that the title suggest that it's an effort to improve private sector information sharing, I believe misses one of the most important parts of the challenge.

For the last 17 years and longer, organizations in the private sector critical infrastructure community have come together in a self-organized and self-governed manner to create value in terms of preparedness, security, and resilience across the critical infrastructure community and inherently the nation. One of the biggest challenges is—and Chris touched on it earlier—that we haven't cracked is the ability for the private sector to receive timely, reliable, and actionable threat information from the government. This is all about risk management, and risk management includes knowledge of threat. What is it that we are going to do to try and address that particular issue?

And secondly, all this conversation about information sharing, what are we going to do with it? The notion is—and no one is having this conversation. It's one thing to create all these streams of data and flows of information, but absent an effective and capable analysis capability that can deliver early earnings to improve detection, prevention, and mitigation, we have really not solved anything.

So I'd be interested in the panel's reaction, one, to how we hope to include a realistic conversation about building out the risk picture to make informed decisions, and secondly, how do we move to a model that will allow us to be able to not just share, but analyze and collaborate in order to improve detection, prevention, and mitigation through early warnings, through identifying patterns and trends of abnormal or malicious behavior and be able to actually move the needle in a positive direction of protection, preparedness, security, and resilience?

TIM ROXEY: That's a good question, Bobs. You hit them in order, right? Threat sharing. What do we do about it? Well, we kind of, you know, work on that pretty much every day, 7 days a week. Threats are identified in the private sector. They're also identified in the public space, as owners and operators of 80 percent of the critical infrastructure. Some of the larger, well-resourced—and it doesn't matter what sector you're in. Some of the larger, well-resourced organizations from coms, IT, utilities, over and over again, we provide information into the federal space for what I call fusion, taking our information, fusing it into classified information, and identifying indicators and warnings, doing the assessment of those indicators and warnings in terms of saturation of the technology and impact to the sector. That's where you get your consequences.

So the consequential component of risk, taking into account the threat and intent, wrapping that together, making actionable payloads and pushing those actionable payloads out to the sector and sharing those payloads across all the other sectors, that, I believe, is taking threat indicator information from the smallest assets to the largest assets, from the most complex assets to the simplest assets, who just got lucky and tripped over an indicator, and fusing that into the larger supplies of classified information. I believe this is the fundamental principle behind the enhanced cybersecurity services construct as well as several others. ISACs, and I would submit certain ISAOs that are well funded and well resources, would be in an ideal place to do that.

Second, bringing a community together, it's crowdsourcing. We in the ISAC, we crowdsource malware to understand its impacts better, so we will share with other people, public and private, within our community that hunk of badness, if you will, to try and understand how it functions the actual indicators that you can tease out of it, what is the subject line, what is the signature down inside. If it's a polymorphic kind of a bug that happens to get loose—and there are many of those right now—if it's something like that that changes every instance that you open it up, those are very, very difficult to detect, but you can detect, however, the consequence. So we can look for places with a consequence and say you have the following, and it will be different on every machine. That's crowdsourcing of that kind of information, which I believe should be something that an ISAO should do as well, but certainly, within the ISAC community, that's something that we try to do.

SCOTT ALGEIER: Real quick, if I may, before you go. I think one of the key challenges we have today—and this challenge becomes even more difficult in the future, is how do we turn the individual initiatives into an integrated capability and how do we turn—we have a lot of one-off agreements between DHS and individual organizations. That's not creating an integrated capability. From a policy perspective, the IT-ISAC remains supportive of the NSTAC Cybersecurity Collaboration Task Force report, which was either 2008 or 2009. I forget exactly what year it was, but that laid a pretty sound basis, a pretty sound strategy for building an integrated industry-government capability. We are part of a pilot program that helped to test whether that capability would work. We found it successful, and we think that there is still merit in that work, and that work deserves to be looked at again through this effort.

MIKE DARLING: Great question. I think it's a very good point. Again, this is the team sport, and the government has to be a partner, not the lead, in assisting and getting that actionable information out. It is a point well taken.

But unfortunately, we are out of time. I very much enjoyed this panel, the opinions. I am certainly better off for having been here and listened to the panel today.

We are going to take about a 10-minute break. We will reconvene for the next panel. So join me in thanking our guest speakers.

[Applause.]

[Break.]

Session I: ISAO Model Discussion

MIKE ECHOLS: We want to continue on with the meeting. Our next participant is Mr. Charlie Benway. Charlie couldn't be here today, but he's on the phone. He is the Executive Director of the Advanced Cyber Security Center. They are an ISAO, and we pronounce it "eye-sow."

Charlie is going to give us some insights on their organization, how they stood up the way that they operate and some insights on this executive order. Charlie?

CHARLIE BENWAY: Thanks, Mike. Can you hear me okay?

MIKE ECHOLS: Yes, sir.

CHARLIE BENWAY: So, Mike, I want to first thank you for the invitation and thank you for accommodating the phone bridge. I apologize I couldn't be there in person, that an emergency came up, so thanks for your patience and accommodation. I really appreciate that.

I've going to talk a little bit about the ACSC model today and who we are and what we do and how we might fit in and view the newest Executive Order. Let me just start with saying that we view ourselves as being one component of this ecosystem that everyone keeps talking about. We don't believe we're the single solution or the single answer, nor do we believe that any organization is, and since this executive order has been issued, it's been very interesting because we have had a number of media outlets contact us and continually try to pin us in the corner with questions of are you trying to—are ISAOs like you trying to displace the ISACs, and our answer to that is absolutely not. That is not our view. That's not our vision. We view ourselves as being complementary to the ISACs, but not just the ISACs, other non-profit organizations and, frankly, for-profit organizations and government agencies. So we view ourselves as a complementary capability that does deliver some additional value into this ecosystem, and we'll talk about that a little bit.

Let me start with quoting a former DHS Secretary, Michael Chertoff. Someone mentioned this earlier today, this morning on the panel, and he says that there are two types of organizations, those who know they have been hacked and those who don't. Our members believe that. As one of the panelists said this morning, sort of the old thought, the old approach of prior defense and patch the holes, that's old thinking. We have to recognize the adversaries are in. It does become a risk management, a threat-based, intelligence-based approach, with resiliency built in, and that all starts with cyber threat information sharing.

So enter the Advanced Cyber Security Center in our region. The ACSC, we are a trusted cross-sector collaboration organized to help protect the New England Region's organizations from the rapidly evolving advanced and persistent threats. When I say cross-sector, yes, I mean across industry sectors. So we have firms represented from Defense Financial Services, biopharma, health care, legal, research, technology, but we're also cross-sector in the sense that we cross the industry, private sector, government sector, and universities, and we bring all of these folks together in our collaboration.

What do we do? We do primarily three things. We'll talk about the information sharing mostly this morning, but I do want to point out that we do also have an R&D and education program and a small policy program that focuses on a couple of specific issues.

From an information sharing perspective, our information sharing program includes several different components. We do do a face-to-face threat-sharing session we call "Cyber Tuesdays." It's every other Tuesday. We alternate the site between the Federal Reserve Bank of Boston and the MITRE facilities here in Bedford, Mass. Those threat-sharing sessions are led by senior Federal Reserve threat researchers, threat analysts, and these are the tactical-level folks from all of our memberships. These are the no-kidding research, threat researchers, threat analysts, network defenders, and I'll include device defenders because that's where we're really moving towards with new technology in the next 5 to 10 years, anyway.

This is not a strategic-level discussion. This is not a session for Chief Information Security Officers. These are roll-up-your-sleeves, hands on, and every Cyber Tuesday, we have the same agenda. We start with a ThreatScape presentation and discussion. That has been a MITRE-provided capability up to this point, although now other members are being integrated into that ThreatScape rotation. We have a best practices agenda item, and then we have an open forum. We also have virtual threat-sharing capability as well as a portal capability for folks to interact.

So we know you can't wait every 2 weeks to hear about the latest threats. That's why we had the virtual threat-sharing capability. It is a STIX and TAXII-based capability. It is currently based on the STIX platform, although we are in the process of looking at what the next-generation threat exchange looks like, and as someone mentioned this morning, not just the exchange of information, but analytics behind it that add value as well.

And is it working? We keep metrics. We survey all of our members, and we keep metrics on how we're doing in terms of our information sharing, and 87 percent tell us they are receiving actionable intelligence not received elsewhere, but it's not just about the actionable intelligence that's shared. It's about the context that comes with the sharing of that information. It's about the ability to reach back to the analysts who provided that threat information in the first place and have a discussion about that, that threat information that was shared, and the why and the who and what was targeted and how is it best detected and resolved.

Now, there are other benefits that come from a regional-based threat-sharing capability, not just the actionable. Although the actionable threat information is important, there are other benefits that come from it as well. Three-quarters of our members say that participation has driven changes or enhancements in their defense postures, and two-thirds say that their cybersecurity professionals developed their skills as a result of participation. And a number of our members tell us that their participation in the organization, they actually use that as a recruiting and retention tool in the tough cybersecurity professional talent challenge, and that that participation provides an advantage over some other folks who are not participating and being able to recruit and retain their folks.

But really , importantly here, in addition to this actual threat information that's shared, it's the best practices that are really key, and a lot of the discussion in the Cyber Tuesdays and some of the other forums—and frankly in some of the virtual sharing too—is centered around best practices. It could be anything. It could be something as simple as who's got the best security awareness program, not just what does that program look like and how do you do it, what are the metrics behind it? What kind of results did you have, and why? What makes a good security awareness program? What's the latest and greatest technology for a particular application, and not only what's working for you and what doesn't, what does your architecture look like? How do you configure it for particular applications or threats or attacks? So there's a significant amount of best practice exchange that takes place as well.

Now, in addition to the Cyber Tuesdays and the virtual threat sharing, we also hold what we call "Cyber Exchange Forums," and, oh, by the way, I should mention in the Cyber Tuesdays and especially at the Cyber Exchange Forums, I think a comment was made this morning on the panel that the Boston group is aghast at sharing information with the federal government. That was an accurate description for a couple of years, and we have been in business now sharing threat information for about 4 years.

Having said that, our members recognize that we are all in this together, and that if we are going to be successful, we have to overcome the speedbumps we have and find ways to share information with the government, and we do have government participation now, but not just share information. One of the folks from the audience asked the question how were we—one of the complaints from the private sector is they don't get timely information or information that' snot already publicly known. That's the criticism, but what we found is, as we've worked more and more with various federal agencies in various capacities, there's trusted relationships

that have developed just like the trusted relationships within the ACSC, and we are seeing greater and greater exchange and greater and greater value.

Good example, this past year, we added the National Guard into our Cyber Tuesday threat-sharing capability and the virtual threat-sharing capability. We have our Fusion Center in the region also participating in our threat sharing. The Commonwealth of Massachusetts is actually a founding member of ACSC, and a number of state agencies participate as well.

At the Cyber Exchange Forum level, these are more—oh, by the way, I mentioned that the Cyber Tuesdays are the strategic level, the tactical folks, the operational guys, day to day. We don't typically have CIOs participating. Every once in a while, we have a CIO stop by, and we had one stop by yesterday. On his way out the door, he said, "You know, I don't come to these that often because you guys scare the bleep out of me," and he said, "What I mean by that is this is my business. This is what I do every day. We're involved in multiple organizations. We get good information from multiple organizations. They all have a value, but I get information here that I don't get elsewhere. It's not like a needle in haystack. It's relevant. It's actionable. It's timely, and I have the ability to discuss it. That's the value here, the fact that I can talk to somebody about what to do with this information."

Now, the Cyber Exchange Forum is another component of our threat information sharing program, and this is a more strategic level. We hold these two, three, four times a year. They are focused on a particular strategic issue. Last year, we did a couple on secure cloud computing. We did a workshop on resilient systems, and we also launched our first or inaugural cyber exercise with ACSC members.

Now, in these forums, this is where we do invite, and representatives from federal agencies do participate, from the FBI, from DHS, from DoD agencies, from a number of different federal agencies, and they all participate not only in the Cyber Exchange Forum on the strategic topics and bringing their perspectives and exchanging best practices, but also participate in the exercises. And I will tell you the exercises with the involvement of the federal agencies has gone a long way to building that consensus that private-public sector needs to find ways to work better together. It was a real eye-opener for several of the federal agencies when we ran our exercises, and they came in with injects, and the private sector really wanted no part of collaborating with those agencies. And out of that came a number of initiatives where these agencies are now working with ACSC on a number of items and working individually with some of the individual members on building relationships, including with the FBI. So it's been a very interesting dynamic.

Finally, as I mentioned, in addition to the virtual threat-sharing platform, we also have the portal, which also allows for interaction amongst members as well.

Now, somebody mentioned the global aspect of cybersecurity and the need for sharing. It's been one of the questions I'm always asked, "Well, is this scalable?" Well, in our view, our vision is, yes, it's absolutely scalable. Again, we are part of an ecosystem. Our vision includes

the standup of other ISAOs, the development of existing ISAOs, and the greater capability, and federating our threat sharing with those other—not just those other ISOs, but with ISACs, with government agencies, and then perhaps scaling on an international basis.

We have met with—along with MITRE, by the way, partnered with MITRE to support the stand-up of similar organizations across the globe, here in the United States in Cleveland and the Pacific Northwest and Virginia and Georgia, a number of places, but also Great Britain, South Africa, Singapore, and several other countries as well. From our perspective, these are not competitive—these are not competitive organizations. These are complementary organizations to partner with and build that federation over time, and by the way, most of the companies that are involved in ACSC are global players anyway.

Now, there's a couple of things on a broader scale in terms of legislation and regulation I think that are going to need to happen to enable that, but we'll save that conversation for another day.

For us, one of our major objectives is the information sharing program. That's really our bread and butter today, but I mentioned we also have an R&D and education program. So we have the major universities in the area, which is a significant strength here, active in the ACSC, and they're active in two ways. Their IT departments and security departments actually participate in the threat sharing and have gained some significant value in terms of support from other more mature organizations in the area when they are under attack in terms of the cyber exchange information, that exchange, and in best practices in a number of other ways. But we also tap the academic and research sides of the universities. We have a couple of small research projects ongoing that are funded by our industry members. One is taking a look at the risk optimization in cybersecurity, and really what it's going is looking at the financial sector and saying is there anything we can learn from the rigorous financial management risk models that we can apply to cybersecurity and build a framework for a rigorous cybersecurity risk management model. And the other is data sharing and the ability to detect anomalies where the universities believe they've got some research that is very valuable in the marketplace today in terms of identifying anomalies.

Now, going forward, we have a major initiative that we're launching, which is an R&D consortium, which is made up of the universities, industry members, and government. It's to bring together multiple universities with grad and postdoc students supervised by faculty aligned with industry professionals and aligning research with industry needs and funding that in a significant way over time and eventually pursuing federal research funding for the effort as well. One of the first steps in that process is the launch of a fellowship program where we're matching both grad and postdoc students, but early career cybersecurity professionals in industry and selecting the top talent and running them through a fellowship program, which includes both curriculum and hands-on experience. So we're pretty excited about the R&D program, and again, I present that to you as, yes, we're an information sharing organization, but it goes beyond just the sharing of information.

Finally, I mentioned the policy area where our members are primarily interested in two things, uniform breach notification standards and liability release, and when I say liability release, our members are not suggesting like seems to be portrayed generally in the media. It's not an issue of liability for erroneously releasing privacy information. Their larger concern is if I share information with you, if you act on that information and your act causes some damage or harm, I don't want to be liable for that. That's the kind of liability relief they would like to see to open up information sharing even greater.

Our view of the Executive Order is that it's a step in the right direction. We have certainly a longer journey to proceed down here, but we do think it's a step in the right direction. We think that where we can help is we can help—I don't like to use the term "standard." It makes the hair stand up on the back of my neck a little bit, but I do think that we could be very beneficial in helping to establish criteria, if you will, for ISAOs and a framework for ISAOs that want to stand up or develop a current capability.

MIKE ECHOLS: Hey, Charlie?

CHARLIE BENWAY: Yes.

MIKE ECHOLS: Let me cut you off there. We've run short of time here. Do you have a closing statement?

CHARLIE BENWAY: Sure. So I think we can help by supporting whatever standards organization is stood up, not just in terms of information standards like STIX and TAXII, but also things like governance, operational procedures, legal agreements, which we already have in place, and I think that's where we can support the Executive Order.

But again, my main point is there are different models out there. ACSC is just one model. It's a regional model. There are other regional models. There are ISAC models, and from our perspective, all of these models have value that they can contribute to this ecosystem, and we encourage our members to participate in as many of them as they can to generate as much value as they can.

MIKE ECHOLS: Thank you, sir. We appreciate your input today and your participation. Thank you.

CHARLIE BENWAY: Thank you.

[Applause.]

Session II: NCCIC on Information Sharing

MIKE ECHOLS: Next, we are going to have Mr. Omar Cruz. He is Chief of Cyber Threat Analysis for the NCCIC, National Cybersecurity and Communications Integration Center. Sir?

OMAR CRUZ: All right. Good morning, everyone. Well, first of all, I want to open up today's—I guess my portion of today's briefing saying that I am exceedingly happy, the fact that I am here today, because we would not be having this conversation 10 years ago. I've been in this business about 10 or 15 years in IT and IT security, and no one was talking about us work with the private sector, let's work together to ensure that we all research a common sense and a common goal in terms of defending against cyber threats. So it is personally, professionally a great opportunity that we are actually now embarking on this new journey.

If you go back several years ago, when the conflict situation occurred in 2008, no one was talking about partnerships. You have the government trying to work together with law enforcement and the intelligence community and trying to go out there solo. So there's a couple of events that actually have gotten us to this point, and I want to start with that before I start talking about what we do for information sharing and some of the things that we need to focus on.

As you all recall in 2013, we had the Mandiant APT1 report. This was unprecedented. Now we have a private company going public about advanced persistent threat, which the government had been working in coordination with the intelligence community and the law enforcement community to say, "Hey, we have this threat, and it's really bad, and it has sophistication enough to get into your network and steal your data," and here we are trying to work with the private sector and work with other partners. Next thing you know, boom, years go out, and all of us in the government like, "Whoa! What happened? I thought we were supposed to be doing that?" Now, all of a sudden, we're saying, "Hey, look, we are not going to sit here and wait for you to decide when you are going to hit the trigger. We need information now, and we need to know what are the cyber threats, what can I do about it, how can I protect my network, whether I'm a private bank, health institution, medical facility. It doesn't matter."

We have seen over the past couple of years, since 2013, how the escalation of cyber incidence has continued to go up, up, up, and up. Another example is in October 2014, we had a company called Novetta Solutions who actually went public with saying, "Hey, we know about this espionage group emanating out of China somewhere, and they are doing all of these nefarious things that everyone should know about." So let's just say that this legislation, the authorities that we have been given at the NCCIC, has definitely opened the floodgates for us to actually start talking, start communicating, and start sharing information in a timely fashion. As you can see, I am excited about that from the beginning.

So a couple of things that we have to consider when it comes to essential elements and information sharing, regardless of the sectors. I am not going to be so specific. I am not going to talk about, "Well, thank you for being here, private sector." It's just across the board, whether you're government, law enforcement, private sector, or international community. The cyber information has to be—you have to be cognizant of the audience that you're reaching out to, the production, the content, the mechanism, and the assessment.

On top of that, we need to ensure that the information must be timely, accurate, relevant, substantive, and actionable. If all I send you is a report with 20,000 IP addresses, it doesn't tell you anything. It doesn't allow you to do anything, but if I can do some level of analysis with some threat information and actually synthesize what's going on with that activity, give you more context, now you can make an intelligence decision within your respective organizations as to what kind of measures you may want to pursue in place.

Now, we the government or the NCCIC may say, "Well, you should follow these kinds of measures and these steps," but you may have a difference of opinion. But you should know how we arrived to that information, how we arrived to that conclusion that if you follow this set of guidelines, you will be protected from any adversary targeting your network. So that's one of the things that needs to happen. Again, cyber threat individual must be timely, accurate, relevant, substantive, and actionable.

The speaker before me said before, what I hear all the time is, "Great. You are reaching out to me. I'm going to work with you, but we all know what happens. I give you information. I don't hear back from you. Thirty days later, it goes into a black hole." So we are trying to change all of that. We are trying to change all of those situations so we have a team, equipped and prepared, be able to ingest the information, be able to take action with the information and share the information in a timely fashion. I am going to talk about how we do that further down within my briefing, but I want to first start talking about what we need to do with the cyber information.

Also, we need to be able to collaborate with public and private sector partners in coordinated response, so it's no longer a government federated approach, it's not a partnership approach, because we do understand how valuable working with the private sector actually is to the greater good of what we're trying to do here.

Watch for and warn about emerging cyber threats. Don't just hold the information until you see something actually occur. If we at the NCCIC have indication that a cyber threat actor may be positioning himself, or country, team, whatever, to carry out some level of attack based on indications that we have received and perhaps in coordination with the intelligence community, we should be able to have this little—everybody come together, "Let me give you an update of what we're seeing. Let me give you information as to what we're trying to do," and now you're part of the conversation. That didn't happen last year.

Last year, in late 2013, it was with the government at the NCCIC, we're working together with all the critical partners, and then when we were ready to take some action, then we will notify you and say, "Okay. So tomorrow, we're going to do this." Wouldn't it be great if you would be part of the conversation and you would be sitting at the same table with the folks that actually are analyzing and looking at the threats before we go public with the information? That would be awesome, and that's what we are trying to do. And I believe the ISAO is going to try to ensure that we get as integrated as possible, so that way you're also part of the decision-making process.

So analyze and mitigate cyber risk to the nation, and that's the common goal. That's what we're all trying to do.

You all heard about the Premera incident yesterday. Two weeks ago, it was Hampton. So we see a pattern. We see a trend here. Last year, it was a major campaign against the banks with their denial-of-service attacks. Every single year, every single month, you are going to continue to see these developmental cyber threats from across the broad—in a very broad spectrum.

So how do we receive information? Not everyone has the same capabilities. Information is provided to us from cyber threat indicators. That could be a malicious payload of a malicious file. It could be an IP address. It comes to us in a number of ways because you're going to send it to us the way you have it. You are not going to change your infrastructure in order to cater to how we can receive it. You are going to give it to us the way that you are already decided that you are going to do it within your environment and your organization. So we have to be able to position ourselves to be able to ingest it, whichever way possible we can receive it, and then make sense of that by doing the analysis that we need to do with that information.

You may give us digital media, malware, like live malware that you caught on your network. We need to be able to receive that information and actually been able to do that level of analysis. Wouldn't it be great if you give me some malware you found on your network and I can analyze it, and we can compare our notes, we can compare our analysis? Your analyst may have found something, but my analyst may have found something different. So now we can actually then group together and say, "Hey, this is your analysis. This is mine. What did you do that I did not do, so we can now further enrich the outcome of what we are working together for?"

Then the reports and analysts, again, it is not just sending you a report that simply says, "This is a bad thing, and you should know about it," but the analysis around the activity. If I just gave you a piece of malicious code that says this file is bad, you are going to look at me and say, "Okay. Thank you. I guess I should notify my IT company that they should take some action," but wouldn't it be great if you knew specifically what the malware does? Once you execute this malware, what is it going to do on your network? Where is it going to go? What is it looking for? Does it need credentials? Is it going to escalate credentials? Is it going to look at your network? Is it going to map your network? Is it going to extricate data? All those activities and all the information analysis-wise should be part of that communication, so you guys are able to ingest it and be able to have much better information.

One of the challenges of information sharing is that everyone is looking out for their own specific areas of responsibility—let's call it that, right?—or mission space. In our case, network defense as the NCCIC, that is our major responsibility, so we're looking for to disseminate that information and ensure there is a timely release of information. That's what we're here to do, ingest the information, do the analysis, and then be able to disseminate it broadly, so everyone can protect against whatever cyber threats that we're talking about there.

But when we start talking about working with the law enforcement community and Department of Justice, for example, the concerns are to identify criminals and then also to preserve evidence. So we're all looking at the same threat actor, different angles completely. If we work with the intelligence community, which more than likely we are, then they are looking for attribution, who is behind the attack. Is it a foreign nation? Is it a criminal? Is it a hacktivist group? Who is behind the activity, so they can better ascertain who is a threat actor, but I'm not so much concerned about a threat actor. I'm concerned about mitigation, containment, eradication, and ensure that I can bring that network back to a health status.

And then, of course, working with the national defense or Department of Defense, they are looking to defend the nation and protect the military networks. So now you have a conglomerate of teams in one operation center, which is the NCCIC, and you have your law enforcement. You have your intelligence, and you have your Department of Defense folks, all sitting in one area, and we are all trying to work together to ensure that even though you have your mission area and even though you have your points of view as to how you want to approach the activity, I from the NCCIC or we the NCCIC need to be able to ingest that information in a timely fashion so we can then analyze it and disseminate it across all of our partners and constituents, whether it's the private sector, critical infrastructure, international community, and so forth.

So let's just say it's not as easy as it may seem when you say information sharing because you have to go through those hurdles in terms of, "Thank you, DoD, but I kind of needed that yesterday, not today. Can we work together now to ensure? Because I want to let you know what I care about, so that way you can clue me in now instead of later." So those things are those challenges. It's a cultural thing, so it's not going to happen overnight. The intelligence community works in a different mindset that our computer network with defense does, so they are going to look for computer network exploitation and protecting their secret sauce of how they operate. But we have to ensure that we work together because I want the information quickly, not later. So we are working to go through those hurdles and ensure that we go past that cultural mindset and start thinking about defense of the networks and then the constituents that we're protecting and trying to achieve information sharing.

At the same time, we all know that the moment you have an organization—and specifically a federal organization like the NCCIC—working with the intelligence community and other critical partners, there is something called classification. Of course, a lot of the information, they are going to be safeguarded on some level of classification, whether it's top secret, secret, and so forth. At some point, we might have to wait weeks or months before that information can come down at an unclassified level.

So we also have to ensure that we are cognizant of the fact that if information was entrusted to us in an unclassified manner, that we're not going to post it on Google, it's not going to show up on Yahoo, but it's actually going to be between me and you as the partner that I'm working with. To ensure that we do that, we use something called a Traffic Light Protocol. I'm not sure

how many of you here today are familiar with the Traffic Light Protocol. Obviously, I won't be able to go in depth because of the time constraints here, but I encourage you to go to us-cert.gov/tlp, and it will give you the actual description of all the different types of colors that we use in order to safeguard and protect unclassified information. So, again, the Traffic Light Protocol is exclusively for the protection of sensitive information by building guidelines on dissemination. We have the colors of red, amber, green, and white. If you 're a private company that I'm reaching out to because you may have an incident that I just became aware of, I may give you that information at the TLP red level because you are the one that is the victim, and you are the one who needs to take action immediately. But everyone else who is part of the community, I may be able to share it at TLP green level, so that way everyone knows something occurred.

Yes.

ATTENDEE: What do you say that Traffic Light Protocol is the biggest obstacle to information sharing? You can't share anything—you can't actually action on anything that's red. You can know about it, but you can't do anything with it in your organization.

OMAR CRUZ: I disagree with that assessment because the information owner is the one who owns the information. If I receive information about a threat targeting your specific company and you say, "Hey, I want to share it broadly with more people," all I have to do is go back to the source and say, "Listen, thank you for sharing it at this level, but based on this mission need, we need to be able to spread the word more broadly." So I hardly have seen a case where that has been denied, and perhaps the channels that you might have gone through have now understood the process, the way it is supposed to be.

ATTENDEE: Well, I have talked to people in ISAOs who say—or ISACs, I should say, the majority of traffic they get is usually at least amber, and as a result, there is not nearly as much dissemination as there could be because the natural tendency is to, "Oh, this is highly specialized information. We've got to protect it." So, in other words, the Traffic Light Protocol ends up inhibiting rather than implementing.

OMAR CRUZ: Those are very good points that should be brought up when we have the ISAO meetings, so that way we can address them now, because, like I said, from my point of view, from the NCCIC, and the way that we disseminate information, if it is at amber level and you as an organization have a need to disseminate broader than that, all you have to do is let us know, and we will be more than happy to go back to the source and provide you the information and give you the approval.

At the same time, we're not trying to inhibit. That's not the purpose. The purpose is actually to disseminate information in a timely fashion and safeguard in the way it is protected from public disclosure. Again, we don't want the information, even though it's unclassified, to be out there everywhere, because then we're tipping off the adversary, and if the adversary knows that we're tracking and monitoring and we're doing activities against them, then guess what they

are going to do? They are going to change their techniques, tactics, and procedures. They are going to change how they do things. So if they were spearfishing you today, since you posted the information on Google and everybody knows about it, then more than likely tomorrow, they are going to SQL injection or cross-site scripting or some other mechanism to be able to get back in it without using the same form of mechanism.

So very good point and very good criticism. I like that a lot, and we are going to be able to capture that when we have the meetings at ISAO and say, "Hey, how can we better ensure that the process to ensure that we are now part of the dissemination?" what it is to provide a mechanism for those recipients to get back to us and say, "Hey, thank you, but I want to do more broader than that," or, "Can you give it to me at a green level, so I can be broader?" or, "At which point can I go white, so that way it becomes as public as possible?" If the issue is that we need to provide a mechanism to have that two-way street, than that's what needs to happen.

Again, working together, information sharing, and of course, the mechanisms in place to be able to safeguard the unclassified information.

But now, if I'm reaching out to you and saying, "Hey, you should work with us because you are going to be able to receive threat intelligence information," then I'm sure you as a company may want some level of protection, and so we also use the Protected Critical Infrastructure Information, or PCII, which is what allows companies to stay anonymous as they work with us. So we will never, never go out there and say, "Yes. Company X gave me that information," because under the PCII guidelines, I'm supposed to protect your identity and the identity of your constituents. Do you can work with us, and your identity will continue to remain anonymous, so that way the sharing of information stays reciprocal without anybody knowing where we received the information from. That is the reason all of our products say at the beginning of the sentence, "From a trusted third party, we learned this bad thing just happened, and you should know about it. And here is all the information about this bad thing that just happened," because we're never going to be allowed to release that information.

There's also concerned about privacy. If you give me information about a threat report or a threat activity that you are looking at, there's also concerns about privacy. So you may be concerned that the fact that you share information with me could be requested under the Freedom of Information Act. So under the PCII guidelines, it is protected from FOIA. So no one would be able to FOIA me and request that I provide who gave me the information.

I'm wrapping up. One more minute.

So in order for us to facilitate currently, as we speak, all of the activities that we do with the private sector companies and the constituents that we have, we have two special programs, you guys have already heard about, more than likely. If not, I'll speak to them real quick, which is the CISCP, the Cyber Information Security Collaboration Program, and the ECS program, the Enhanced Cybersecurity Services program. If this is the first time you are hearing about it,

these are two programs that we have that allow us to collaborate legally, legally allow us to collaborate and share information in a timely fashion at the analytical level, not at the management level, not at the director level, not at your lawyer level. This is at the analytical level. So that way, we remove from the equation all the suits, and we allow the analysts that wear the sneakers and the jeans and the T-shirts to work together. And that's what they do. They are allowed to be able to do analysis or real-time threat information and be able to get back to you through meetings, through collaboration, letting you know what we found. We have a malware lab in our building that allows us to ingest information, analyze it, and give it back to you in terms of the results of our analysis. The information that you share with us allows us to then generate the necessary threat reports—or alerts—let's call them that—that we can then disseminate broadly, using, of course, Traffic Light Protocol, and providing the information to all of our constituents, private sector, international, federal, and so forth. So those two mechanisms allow us to do that.

In the case of ECS, now we're sharing classified information with private companies, and by doing so, we are able to provide information in a timely fashion as opposed to wait for a downgrade request that could take weeks to happen from that source. So if the information came today, fresh out of the oven, we can provide this information to those companies that are part of the ECS program, and they are able to receive it today as opposed to waiting a couple of weeks before the information comes down downgraded. The difference is because I am able to re-ingest the information in a classified fashion, then they can receive it in a more timely fashion. Once the information does become downgraded, than obviously we are following our normal process of dissemination broadly to all of our partners and constituents.

I wish I could speak more. I could speak on and on about this, but unfortunately, I have the tall man here looking at me, which I guess that means I'm done. It's been a pleasure, and I hope this information has been informative to all you all. Thank you.

[Applause.]

MIKE ECHOLS: Thank you, sir. The one theme that I want to become clear is that we have heard criticisms about the government not working together. I work with these guys very closely. Just as we are trying to get a better relationship with industry, we are trying to get a better relationship within the government. So we work very closely on a daily basis. These are not individual efforts that are occurring.

Session III: Automated Information Sharing

MIKE ECHOLS: Our next partner to come up is Preston Werntz. We work very closely with Preston. He is going to speak on automated information sharing. Preston is the Chief of Technology for the NCCIC.

PRESTON WERNTZ: Thank you, Michael. Good morning, everyone. My name is Preston Werntz. I work over in the NCCIC, and I am going to talk a couple of minutes about a new

initiative. It is actually automated indicator sharing, some of the recent administrative, legislative proposals, kind of tag the NCCIC as that portal to interface with private sector for cyber threat information sharing. One of the things it specifically requests out of the NCCIC is a near real-time ability to share cyber threat indicators.

What we have started to do now is put in place a program over the next year or so to introduce some capabilities to do that automated indicator sharing, and the key really here is for the NCCIC, to the fullest extent possible, automate the ability to receive indicators, filter them, analyze them and dissemination them back out, with a focus on private sector indicators into the NCCIC being shared back out, then across Department's agencies, and at the same time identifying additional government data to get that shared back out through the private sector.

Some of the technology pieces of this for us are the STIX and TAXII protocols. I think most people here might be familiar with them. STIX is the Structured Threat Information Expression, and TAXII is the Trusted Automated Exchange of Indicator Information.

Omar introduced the CISCP program, for folks who are not familiar with it. Right now, we share cyber indicators with CISCP partners. We share in STIX format along with traditional PDFs, that that STIX content right now is being e-mailed out. It's being uploaded to portals. It's not really at machine-to-machine speed, fully automated. We have been running a pilot for about a year to do this, and hopefully, before RSA, we are going to stand up a TAXII server out in a fed ramp cloud environment to allow us to share additional STIX content through that TAXII server, both out —cyber threat indicators we get in from CISCP partners. Right now, within DHS, we turn that back around. We do some sanitization. We do some redaction of data, anything that is personally identifiable information that's not really important to understand the cyber threat. We kind of strip that out, mask it, send it back out to our partners. That gets back to what Omar talked about, about getting stuff down to a TLP green or TLP amber.

One of the keys here for us now is with the—once we have the TAXII server, we'll be able to share that faster out to both private sector departments and Department's agencies and also international partners, I should add as well. This first phase will be DHS pushing out that STIX content via TAXII through that TAXII server out in the fed ramp cloud. Before the end of this calendar year, we are going to be introducing additional capabilities to allow us to do that automated in just as well. As prior sector partners and other Department's agencies have TAXII capabilities, they can start pushing us STIX content into DHS. We will be looking to introduce commercial or other capabilities internally to help us do the filtering on that, do the analysis, redact or sanitize, PII, PCII information, that kind of stuff, so we can turn around and share it back out much faster.

Kind of FOC, the final operating capability, we are targeting early 2016 to have that in place for that full loop. Like I said before, RSA will start to push out STIX content, and right now, we are looking at addressing some of the internal policy issues. One of the things we'll be doing soon in the next couple of months is coming back out with some guidance to our private sector partners saying, "Hey, here is how we would like you to kind of—if you are sharing indicators

with DHS and if they are in this format and using these fields, here are the privacy implications if you share this data with us, and here is how we are going to strip it out. Here is how we are going to redact it or sanitize it. If you don't share it with us, it's even easier. We obviously need some of this to understand the cyber threat, but certain pieces, we don't need to understand the cyber threat. Don't even send it to us. It's less work for us to strip it out."

Like I said, internally, then we will be adding those capabilities to help filter that out, help do some automated analysis, so obviously requiring human analysts to make tougher decisions on edge cases, things like that. But the more we can analyze in an automated fashion and turnaround fashion, obviously we are going to speed that cycle up.

Omar touched on the speed at which we are sharing is not always optimal, so this is an effort by us to kind of reduce that time from receipt all the way back out to disseminate.

Like I said, we will have a TAXII server stood up hopefully by RSA with pushing out for folks who are already in the CISCP program. You will see more about that as folks get TAXII capabilities. It will be easier for us to share, and one of the reasons I'm here, as we figure out what ISAOs are going to look like and how they are going to share with DHS, this will have an impact on where this kind of sharing program goes and how we're going to touch ISAOs with those member companies behind them over time.

Key takeaways for just a couple minutes here is we are moving out on this automated indicator sharing activity. TAXII service set up RSA, pushing out DHS, STIX content. Before the end of the year, the ability for a private sector and other Department's agencies to push STIX content to DHS, and then by early next year, we should have kind of a full operating capability where a lot of the manual processes, we're still going to have to do. We're going to be introducing other commercial capabilities then to help that to fully automate those processes. And one of the last things we're looking to do into next year is to stand up kind of a shared services capability, more geared at Department's agencies, obviously across the federal departments' agencies, a lot of different maturity levels on technology and ability to do this. For agencies that have less capabilities, DHS, we're going to look up a shared services capability, so agencies can kind of plug in and get access to that STIX data via TAXII without a lot of investment by them. So those are just a couple things I want to kind of hit quickly.

And I will stop at this point for questions for myself, and I guess I'll turn it back over to you, Mike.

MIKE ECHOLS: Sure. Go ahead and ask.

PRESTON WERNTZ: So questions?

Open Floor Comments and Questions

MIKE ECHOLS: So the floor is open for questions in general or for Preston. With that being said, there are some questions that we may not be able to answer. However, for the record, go ahead and ask them.

PRESTON WERNTZ: Yes.

ATTENDEE: How would you say your mission and capabilities is intersecting with the more cross-domain hazards and requirements that we have heard today?

PRESTON WERNTZ: We will be touching on a lot of that. Certainly, within DHS, within my part, within Cybersecurity and Communications, we work very closely with the infrastructure protection folks. So, for me, what I'm talking about here with an indicator sharing, this is our first kind of foray very specifically on indicators. As we get this capability in place, it's going to grow more broadly, and we're going to tack on those other pieces of the cyber mission, which we will then kind of touch and overlap that physical side in that all-hazards approach, because, obviously, part of the NCCIC there is—you know, a lot of people at the NCCIC and C-Cyber, but there's a lot more to the NCCIC, especially on the communications side and national security emergency preparedness communications, and folks sometimes initially see. So that certainly is things we are talking about, looking about on the control system side and the communications side, more broadly than just very narrow cyber.

ATTENDEE: Two questions, one for you and one for Mike.

PRESTON WERNTZ: Which one is the hard question?

ATTENDEE: His is probably harder.

PRESTON WERNTZ: Perfect.

ATTENDEE: You used a lot of acronyms, and since I'm not a roll-of-the-sleeves techie grunt, where do I find out more information on all the acronyms you used? Is that on your portal at NCCIC? Is that a portal at US-CERT if I wanted to analyze what all these acronyms mean to get a better understanding?

PRESTON WERNTZ: I think on the US-CERT side, they've got most, and I'm not sure if we're sending our materials as a follow-up to this.

MIKE ECHOLS: Yes. They have most of those terms at US-CERT.

PRESTON WERNTZ: Okay. Yes. The us-cert.gov portal, it's going to have pretty much all of these, especially on the CISCP side and the Traffic Light Protocol stuff and STIX and TAXII.

ATTENDEE: Okay. And then a question for Mike, I had asked a question earlier, and you told me to wait. If I read the Executive Order in terms of the SO, it talks about DHS entering into an

agreement to a competitive process. As a lawyer, agreement to me means contract, but then I heard when we were talking on one of the panels about feds at the table and somebody says, "Well, no, this isn't a contract. This is a grant program, not a contract, and it is going to be grants," to me, it sounds like something is going to be money to do something, like a grant for my kid to go to school. And I think you used the term "grant." Clarify for me. Is this a contract, a grant? I'm still confused on the nature of this vehicle that's been set up here.

MIKE ECHOLS: We propose to deliver a cooperative agreement. Our contracts people tell me that there's a difference in language when you are talking about procurements and when you're talking about giving out a grant or a cooperative agreement. The grants processed is managed by the DHS Chief Financial Officer office, and so, as such, we are going to follow that process. That process essentially—there's not an RFI or an RFP. A document of a funding opportunity is posted to grants.gov, and essentially, we tell you what we're looking for, the outcome we're looking for, and you tell us how you would do it.

PAMELA WISE-MARTINEZ: Are you open for comments now?

MIKE ECHOLS: Yes.

PAMELA WISE-MARTINEZ: Okay. Good morning. My name is Pamela Wise-Martinez, and I am representing the Office of the Program Manager for Information Sharing Environment. We are actively involved in improving cybersecurity information between federal agencies, state and local governments, and with private sector. Our office leads or co-leads three inter-organizational groups that have knowledge and expertise to offer on how to implement this Executive Order, so that's one thing.

The first group is the Information Sharing Access Interagency Policy Committee, comprised of federal agencies, focused on improving terrorism and homeland security information sharing. The second group is the Standards Coordinating Council, a public-private partnership comprised of federal program representatives and now government standard organizations, and the third and final group is the Interagency Committee, comprised of federal agencies, exclusively focused on improving cybersecurity information sharing.

Various components of DHS are involved in all three of these groups, and we work with DHS Capstone Information Sharing, Safeguard and Governance Board, to ensure coordination and unity of the effort. We believe this is important for the execution of the Executive Order 13691 to not only improve cybersecurity information sharing, but also continue to combine cybersecurity and non-cybersecurity, as we spoke of earlier today, non -cybersecurity information to enable more holistic, integrated, and interoperable assessments in response to all types of threats, risks, and hazards.

We also believe that there is a great potential to leverage the nation's previous investments and responsible information sharing to improve cybersecurity sharing, and finally, we commend DHS for leading and planning for implementation of this important Executive order and look

forward to submitting more extensive comments after this meeting for more information, and I will provide you a copy of this as well. Thank you.

MIKE ECHOLS: Thank you, Pamela. Any other comments? Sir.

ATTENDEE: I don't have a comment, not coming from the illustrious organization like the ISE. I do have a question on the automated STIX and TAXII server. Can you just tell us a little bit about how much you will be able to automatically actually ingest those threat signatures and get them out? I mean, there is going to have to be some kind of manual analysis to at least verify the information and verify that the PII has been stripped out. Isn't that the case?

PRESTON WERNTZ: And there will be. One of the things we're doing now is we're sitting down with our internal privacy and policy folks to look at the indicators we get in and build some matrices. If an indicator comes in of a certain type, if it's just malware hash, if it doesn't have an e-mail address, some of those things become very easy to automate because there's less risk. Depending on the data you send in, there's a more risk, and that's where we're going to be working back out, hopefully with the private sector, and say, "Hey, here is some guidance. If you are going to send us an indicator, a spearfishing indicator"—and within the STIX profile we use for indicators, we're going to push out a data dictionary that says, "Here's the 15 fields you can send us. If you send us three or four fields, these have more privacy implications." So if you can make sure before it comes to DHS, that company, that ISAC, that ISAO has already kind of stripped some of that off, it makes our job easier. And if not, we're going to have to build some of the business rules to make sure we take care of that PII and don't share anything that's not really required to understand the cyber threat. But then internally—so, internally, then it is on us to have those guidelines in place of how we're going to share it, what fields we're going to use, and then we have our own internal kind of oversight and auditing purposes to make sure as we share the stuff out, we're keeping an eye on what's going out.

ATTENDEE: So, obviously, a to field, right, would probably be PII, you would want to strip out, except for the fact that the two-field could actually reveal something significant about the campaign. So how do you deal with that? Also, how do you verify? How do you differentiate at an automated level, say from the to field and the from field? Because the from field, obviously, is going to contain information also about the campaign, its origin, and the fact, the from field's spoofed origin can contain PII, but likewise be significant. How on earth do you untangle all that?

PRESTON WERNTZ: And that's what we're working through now. Certainly, within the STIX, the way it's laid out in STIX when we use like the observable, stuff like that, it's very easy for me to break out and say, "This part of the xml is the to. This part of the xml is the from." I can throw some machines and some scripts at that, so I don't confuse the to and the from. But we're going to have to make some decisions internally. So you know what, the from field is more important to understand the cyber threat because of that spoofed address. If the person is going to a particular company, that's where we're probably going to make the determination and say, "You know what, that is not really important to send out." It might not be helping you

understand that broader cyber threat. So, therefore, we're going to redact that or sanitize that, but those are things. We're going to put out our thinking on what that guidance should be and those policies and examples out to private sector and say, "Here is what we are thinking," how do we get that feedback from folks across the ISACs and ISAOs at that time to say, "Does this make sense? Does everyone kind of agree, these are the right ways to tackle this?"

ATTENDEE: Thanks.

ATTENDEE: Question. Chris Castelli with Inside Cybersecurity. Mike, a question for you about the grant process. Any timeline as far as when we'll see the notice posted?

MIKE ECHOLS: The message that we're delivering to everyone, because the same message has to go to everyone, is sometime in the late spring, we're expecting to put out the announcement, and sometime in the early fall, we expect for the standards organization to be up and running.

There is one area that I wanted just to clarify also. We all know that there are legislations up on the Hill related to ISAOs, and with our effort and everything that we're doing, if a law is created, we will then implement whatever dictates that law provides into whatever we're doing. So there could be a course correction in the middle of our effort. It will be based on there being a law passed.

Anything else? Got one more, and then we'll call it a day. What I can tell you guys is 24 hours a day, 7 days a week, you can provide comments, insights to isao@hq.dhs.gov.

CORY CASANAVE: I just had mentioned very briefly before, there is a current international standards effort for risks and threats. This is being conducted in the Object Management Group to bring together the multiple domains and formats. Good work that's been done, for instance, since STIX and TAXII, it's been done in NIEM. It's been in Emergency Management in Oasis, so that we can fuse this information together and understand how we can share it, how we can federate it, how we can analyze it. This is an ongoing standards effort that is intended to connect them, not provide something that replaces it, not to make one ring to bind them all. So we just want to make sure that this community is aware of it, is invited to it. You can go to Object Management Group, omg.org, to find out about it. There is a meeting next week in Reston where it's going to be discussed in detail, so we just want to make sure that you are all invited and welcome. Thank you.

Closing Remarks

MIKE ECHOLS: All right. I want to thank you all for coming today. There will be several more workshops. What I will invite you to do is to send me a message personally or to the ISAO mailbox, and if you have a suggestion or an insight—not saying that we will take it, but if you have a great idea for a workshop that supports this effort, please let us know. Thank you.

[Applause.]