Information Sharing and Analysis Organization (ISAO) Workshop
Tuesday, June 9, 2015
VOLPE Center, Cambridge, MA

Opening Remarks

MIKE ECHOLS: Okay. Good morning. Like all good security meetings, we need to have a security briefing before we start. So if you could give your attention, we'd appreciate it.

VOLPE STAFF: More of an announcement than a briefing. So my name is Carolee Dresha [ph]. I'm Chief of Safety and Security here at the VOLPE Center, so welcome.

Just real quick, there are three emergency exits from this auditorium, one in the back where you entered and one on each side of the auditorium. If you're disabled, please use the one in the back—these two have stairs—as you exit. In the event of an emergency, you need to exit, please, you know, obviously closest exit and away from the building as far as possible.

When it comes to lunch, there is a coffee shop on the first floor. There's also a cafeteria on the second floor you're permitted to use, and obviously, there's many options across the street. You will be rescreened when you come into the building, but just keep your name tags with you.

Great. Have a good day.

MIKE ECHOLS: Okay. Good morning. Welcome to the ISAO Workshop. We're happy that you could attend, finally. All right? We're here to talk about Executive Order 13691. The executive order was put out on February 13th, 2015. It occurred. We're moving forward. It provides us an opportunity to create a new paradigm for information sharing. What that will look like is highly dependent on the input that you provide, okay?

My name is Mike Echols. I am the National Coordinator for this effort, but I'm also the JPMO Director at Department of Homeland Security, and I have information sharing programs.

Today, we are going to give you some updates on where we are with this process and this project. You are going to hear from some speakers, but the most important aspect of today is your participation. I mean, I look around the room; this is the Who's Who of information sharing. Most of you in your organizations, I've dealt with you for years. You are the right people to help us figure out the path forward.

So we will be in this auditorium until noon. Lunch break is at 1 p.m. There's a 15-minute grace period after lunch, 12 to 1. We'd like everybody to be back and ready to go at 1:15. You'll see that in your programs.

Logistics. The bathrooms are right outside of this room here. Please feel free to very quietly move about as you need to.

Our goals for today, we want to spark the type of conversation that needs to occur to advance this opportunity, and I call it an "opportunity" because, in my opinion, the more individuals that we bring into this cybersecurity game, the greater opportunity we're going to have to win it, okay?

We want to explore some general concepts, models, opportunities. We want to understand the challenges, okay? The idea is not to demean the executive order. It exists, it is, and we're moving forward. The idea is to understand the challenges that we need to overcome to make it live, to make it sync [ph].

We want to take a deep dive into some subject areas through our breakout sessions, and we want to use the data. We're going to create a white paper. We're going to have another session, which I'm going to announce in a minute, at the end of July. From those two sessions, those white papers will be provided to the standards organization. All right.

So relative to our process, the executive order was stood up in February. It instructs us to create a standards organization. That procurement has been put out. I believe it closes on the 17th of July. In that procurement, organizations and entities will advise us as to how they would go about meeting the requirements that are in that procurement. It's on http://www.grants.gov. It's a cooperative agreement. I think it totals to $11 million.

The next session will be in July, in the last week. It's going to be at San Jose State University, and you will be receiving information on that.

I need to advise you all that all conversations that occur in this auditorium will be recorded. They will be put on our website for the public and people who could not make it here so that they will have the opportunity to hear those conversations, all right? We do not intend to put out a list of the names of the people that attended today. If you do not want the name of your organization or entity on a list that we will release, you can opt out. You have a week to send to ISAO@hq.dhs.gov and advise us that you do not want your name or your entity listed there. That's from my Privacy Officer, okay?

Any question with any of that?

[No audible response.]

MIKE ECHOLS: All right. So without further ado, I'm going to bring up Mr. Ben Flatgard. He is going to introduce our speaker this morning, General Touhill. Ben serves as the Director of Critical Infrastructure and Information Sharing on the National Security Council. Introduce yourself. He's new to that role. In this capacity, he is responsible for developing policy that will

enhance cybersecurity and critical infrastructure and increase the effectiveness of cybersecurity information sharing.

Prior to joining the NSC staff, Ben served as the Senior Advisor of Cybersecurity Policy and Strategy at the U.S. Department of Treasury, Department of Commerce, and the White House. And as Ben comes, the last thing I will tell you is tweet #ISAO. We're monitoring that. Any insight, any issue, any problem, any idea that pops up from something that's being said, we want to hear it. So we ask you to tweet, okay? If you're fumbling with your phone, make it count. Thank you.

Welcome

BEN FLATGARD: Thanks, Mike. Appreciate the opportunity to be here with you all today. Good morning. It's great to be here at the VOLPE Center in particular, which advances public-private partnership and seeks to advance learning in all modes of transportation, though given the looks of Boston traffic this morning, there's a lot of work to be done in that field.

We won't spend any time on that today, but we will talk about cybersecurity, and particularly, we'll talk—and I want to spend a few minutes just highlighting the framework that the President has laid out here, which lays the groundwork to create public-private partnerships, importantly, around the field of information sharing and cybersecurity.

So President Obama has been focused on this since the beginning. Back in 2011, you will remember he issued his first executive order on cybersecurity, EO 13636, which amongst other things laid the groundwork and created the NIST Cybersecurity Framework. Just this past February at the White House, the first-ever White House Cybersecurity Summit, President Obama signed Executive Order 13691, which as Mike said started this whole trend toward Information Sharing and Analysis Organizations. The executive order lays out a framework for expanded information sharing, which is designed to help private sector companies work together and work with the Federal Government to quickly identify and protect against cyber threats. The purpose of this order is to create a foundation upon which different communities can and will self-organize. The EO encourages the development of Information Sharing and Analysis Organizations (ISAOs) to serve as focal points for cybersecurity information sharing and collaboration.

Let me tell you four key things that we really hope to accomplish with this EO. First, we hope to make it easier for companies to trust each other when sharing information, private to private, which will expand, hopefully, the scale and pace of information being shared. Second and perhaps most importantly, ISAOs can facilitate information sharing across sectors, from ISAO to ISAO, and regions, preventing information sharing siloes. Third, they provide a partnership structure for DHS and the government to connect with the private sector and to increase the trust and the sharing of information between the government and private sector entities. And last, ISAOs set the stage for future legislation, making key steps, like providing target liability protection, for information sharing more attainable.

Now, established Information Sharing and Analysis Centers should not view these new organizations as competition. In fact, it's just the opposite. We will continue to look to ISACs to provide standards and best practices that will help new organizations benefit from their long history and their significant lessons learned, and as new organizations come online, the entire community should benefit from greater quantities as well as greater qualities of information. Like any maturing ecosystem, established players may, in fact, also find new innovations from new entrants.

So as we continue to work and as you particularly continue to go out and work to enhance information sharing and unite communities through ISAOs, we in the administration are going to continue pressing on Congress and working with them to make sure that we advance information sharing legislation. The administration remains committed to striking that careful balance between facilitating information sharing and protecting privacy as well as civil liberties. We have been dedicated to working with Congress to craft legislation that reflects that balance and at the same time can pass both houses of Congress. There's no doubt that the thoughtful approach taken recently in both houses and by both parties significantly increases the chances that we can pass an information bill soon, which the President can actually sign, and we look forward to that.

So we recently supported two House bills that passed with bipartisan support. Both bills do have pieces that we'll continue to work on, and particularly as these bills move to the Senate floor and the Senate takes up its own version of that legislation, we'll work very closely to make sure that we can get this to the finish line. So we'll have a busy summer in Washington to make sure we get this done. I look forward to having a busy day with you all talking about information sharing and ISAOs.

Without any more time, I'd love to introduce General Greg Touhill. General Touhill has had a very distinguished U.S. Air Force career and recently—well, I guess not so recently anymore—Greg has joined the Department of Homeland Security as a really key leader in information sharing and cybersecurity as the Deputy Assistant Secretary there. So, General Touhill?

Keynote: Future of Cyber Threat Information Sharing

Brig Gen GREGORY TOUHILL: Thanks, Ben. Well, good morning, everybody. Happy Tuesday. I'm sure you're as disappointed as I am that our team scheduled this activity when the Red Sox were not in town.

[Laughter.]

Brig Gen GREGORY TOUHILL: Well, I thought that would elicit a little bit more reaction. Gee whiz. Did everybody get enough caffeine this morning? Anybody missing caffeine need to get a couple slugs of coffee? If you do, please feel free to go outside the room and enjoy your caffeine.

Today, what I'd like to do is I'd like to give you both an educational and informative discussion on information sharing and how we envision the future of information sharing. Andy Ozment, our Assistant Secretary, was originally scheduled to be here today, but frankly, Ben's colleagues scheduled something that he didn't expect to pop up, and he had to cancel, and at the last minute, he told me to grab the flight to Boston and come on up here. And anytime I get to come back to my hometown, this is a good thing.

So, in any case, cybersecurity is all about risk, right? It's not a technology issue. It's not an issue just for the server room. It's an issue that should be a discussion in the board room. It needs to be on every agenda in your companies, but it also needs to be a discussion in every classroom and in every dining room and in every family room because it's a risk discussion for both the home and the office. And as we talk about information sharing, we're talking about not just information sharing for the benefit of our business, our government, and the like. We're talking about risk management across the whole country.

And at DHS, we have three principal missions in our office. The first one is working with the departments and agencies to defend the dot-gov domain, and we do that not only within the Federal Government, but information sharing with the state, local, tribal, and territorial governments to help them get the information that they need, so that they can better manage their risk.

Our second mission set is to help everyone else, harden the private sector, the dot-coms, the dot-nets, the dot-edus, amongst others, and once again, information sharing is critically important.

And then our third mission set is we work with the private sector and other departments and agencies to basically harden and preserve emergency essential communications because without fiber there is no cyber.

So given that mission set, as we take a look at distilling that down, information sharing is a critical component of all of that, and since it's all about risk, what can you do? What can we do to help buy down that risk? Well, as we take a look at all the different things that we see when our incident responders through the United States Computer Emergency Readiness Team and the Industrial Control System Emergency Response Team—when they go out, the CERTs go out, we see a couple of things that I want to bring to your attention that I think will help frame further discussion in this presentation, and it's all about buying down risk. And we see, based upon all the different incidents that we respond to, that you can roughly buy down about 80 percent of your risk through implementation of best practices. "Cyber hygiene" is another term that folks talk about. And as we take a look, when we go out and do incident responses, adversary sets are very diverse, and they can be criminal activities. The nation state actors are very sophisticated and get a lot of press, but there's also just plain stupid that are out there, too, folks that are not configuring systems correctly. You've got insiders who will leverage

different things and weaknesses in the systems that are out there and the like. You can buy down your risk by implementing best practices.

You can also buy down your risk, we estimate, by about 15 percent by information sharing, and that's one of the reasons why we're here. And what do I mean by buying down the risk by about 15 percent? Based upon our analysis and the incidents that we respond to, folks that are going out and looking for certain types of information aren't doing it in a widespread manner. They're going serially, one right after the other, toppling like dominoes. If we can interrupt that domino chain through information sharing, then we can stop all the dominoes from falling, to use that analogy. Information sharing proves—has proven itself time and time again to work.

Many of you in the room have been to other presentations that I have given, and you've heard me talk about the cyber neighborhood watch. Well, I want to foot stomp it again for those who haven't me.

And God bless you for that sneeze.

If we look at cyber information sharing like we would a neighborhood watch, we want to make sure that we minimize the threat environment and we buy down the community risk, and through information sharing, we are indeed buying down community risk because a threat to one is a threat to all, often. And for example, if we were all in the same neighborhood and a guy named Greg goes and breaks into Rob's house, you don't need to know that it was Rob's house that got broken into and the inventory of stuff that Greg took. Rather, what you need to know is that Greg comes in while everybody is at work, broke—defeated the lock on Rob's front door, and, oh, by the way, since it's the same neighborhood, chances are pretty good the builders went to the same hardware store. And you probably have the same type of lock on your front door. You want to know that that lock can be defeated, so that you can buy—you can adjust and manage your risk by use of compensating controls. Get a deadbolt. Change the lock. Get a big hungry dog. You know, there's lots of different things that you can do, but it's all based upon your risk appetite. But if you don't know there's a guy that looks and acts like Greg in the neighborhood, then you don't necessarily have all the information you need. So, therefore, we find that information sharing really does work, and it can help buy down your risk.

Then the last part is that 5 percent, incident response. Chances are pretty good, sometime in your lifetime, you will have a cyber incident. Many of you may be having one right now and you know about it, and some of you may be having one right now and you don't know about it. But incident response best practice is having a plan. Plan for it in advance of the incident. You know, when I talk about it, a lot of folks talk about it, "Give me examples of somebody who didn't have a very good plan and how could—you know, why—why do I need to make a plan in advance?" Do you want to be that executive who has the microphone thrust in their face after an incident and not know what to say? Do you want to be the CIO or the CISO who sits—or stands in front of the board at attention and doesn't have a plan, who doesn't know what the impacts are? I think not. We're finding that folks who have a plan in advance have better

control and can buy down their risk, and this is what we look at as part of the risk management umbrella of activities that you need to keep in mind to buy down and manage your risk.

So there's some tools out there that we've been promoting through the government. Ben mentioned the executive orders. The Cybersecurity Framework has proven itself to be a very valuable tool for most folks, and I would submit to you that it's not just a—you know, at the strategic level, it's not just a cyber risk framework. It's just a great risk framework, period. Identify what you have and what the risks are—threats are to what you have. Protect against those risks based upon your risk appetite. Be able to detect when you're under attack. Have a plan to respond, and build resiliency in. What a great framework! And we're going around the country, and we're working with our partners in both the public and the private sector, with industry and with academia to help promote this framework because it's a great construct for identifying and managing risk.

We're also already sharing information through what we call the "C-Cubed Voluntary Program." Many of you who know me know that I don't like acronyms, and I don't particularly like briefing off of slides either, which runs counter to what most folks believe about military people. But I really don't like acronyms, and I would prefer having a conversation rather than slides. But the C-Cubed Voluntary Program, the Critical Infrastructure Cyber Community Voluntary Program is a mechanism for information sharing, and it's a nascent program. I won't declare victory on this one right now. I think we can do a better job out of—out of everybody in this room and everybody across America to share information. However, it's a great start, and we're seeing some positives. And we are, in fact, getting some good information sharing from some sectors, and we look forward to getting more. But there are vehicles in place, and this is one of the programs that's out there.

And then finally, risk assessments, this is something that we are working with our critical infrastructure partners, and we are sending folks out through our NCATS, our National Cybersecurity Assessment and Technical Services teams to assist with risk assessments for our public sector departments and agencies in the dot-gov space, but we're also working with some of our commercial sector critical infrastructure partners to help them identify some of the threats and their vulnerabilities so that they can better manage risk. And we also have a tool that's downloadable through the ICS-CERT with the Cyber Security Evaluation Tool that has had—well, just this year alone, I believe it's over 10,000 downloads from around the country—to help folks do it themselves, and it gives the listing of kind of a structured question set, answer these questions to help you identify really where your risks and vulnerabilities are. So there's a lot of activities that we were already providing, but there's still some other things that we need to do, and that's why we're here today, despite having some best practices identified.

So when we do have an incident, who are you going to call? Are you going to call Ghostbusters? I don't think so.

All right. So how many folks have heard of the NCCIC before—or actually, how many folks have not heard of the NCCIC? All right. We got one here who has not heard of the NCCIC. All right.

Wouldn't it be cool if you had a national center that was fusing all cyber and communications issues? Well, we got one, and we call it the NCCIC, the National Cybersecurity and Communications Integration Center. It's located in the Metropolitan D.C. Area, and it's one of the teams that I help direct and oversee. And we are open 24 hours a day, 7 days a week. We have the primary location in the D.C. area, but we also have other facilities, backup facilities elsewhere in the United States so that we can provide continuity of operations. And our mission, as I mentioned, you know, the three main points: defend dot-gov, harden everybody else, and preserve emergency essential communications. And we are deeply involved with incident response, incident information sharing, analysis, and the like.

Many of you have seen some of the products, such as our malware indicator finding reports, or MIFRs, our joint analysis reports. We work with our partners in law enforcement, such as the FBI and the Secret Service, to do joint products, joint information bulletins, and the like. As a matter of fact, we have partnerships where we, out of our team, send liaison officers to the NCIJTF, the National Cyber Investigative Joint Task Force. And I believe, John, you may be talking about that later today. And we also have FBI and Secret Service agents involved in the NCCIC on the floor as well, so that we have information sharing with the law enforcement community as well as others.

In the NCCIC, we have representatives from different departments and agencies, from the Information Sharing and Analysis Centers, from public and private sector partners from all over the country. Not everybody is on the floor at the same time. Folks come in and out as the mission dictates, but it's the shared situational awareness, and it's a focal point for information sharing between the public sector and the private sector.

We have two operational teams that are operating out of the NCCIC. The first is the United States CERT, and I know you can read, so I'm not going to read the acronyms out to you. The CERT focuses on doing all of the different analysis and deep-dive type of stuff for common systems, you know, network systems, desktop systems, and the like. These are the incident responders who you hear about in the newspapers often when there's a very big breach. They're also operating the Einstein suite of systems, which is the National Cybersecurity Protection system, and because they're actually operating a system, they're called a "readiness team" as opposed to a "response team."

But because industrial control systems, or SCADA, Supervisory Control and Acquisition—what is it? I forget what the acronym is because I'm an acronym jihadist. I hate them. The SCADA systems. Industrial control systems were increasingly vulnerable to attack and exploitation. So a couple of years ago, the Department invested time, material, and manpower to standing up a separate team just for industrial control systems, and we work with the manufacturers and the operators of industrial control systems around the county and around the world to try to harden up the industrial control systems. Let me tell you, this is something that keeps me up at night, and information sharing within the industrial control system community is critically important, and we tell people avoid connecting industrial control systems to the Internet as

much as possible. But these are tools and the resources that we've invested in incident response, and unfortunately, these folks are very, very busy, as you can well imagine.

So you can read this slide, but for those folks who are on the recorded version, I'll read it out loud: Why do we care about information sharing? Well, frankly, we all should be caring about information sharing, and that's why you're here. But as I mentioned, the NCCIC is the hub of information sharing, and the reason being is, like a lot of different activities, everybody in the Federal Government is very interested in being helpers. But we can't afford to have different messaging coming from different activities. We have to be speaking with unity of effort and unity of messaging, and frankly, when it comes to information sharing, it's important to make sure that we have the most contemporary, the most current, and the most accurate information for the public as well as our fellow government partners. The NCCIC was created to do that, and we are working with law enforcement, the intelligence community, private sector, and Federal Government agencies all in one place, so that we can in fact effectively communicate with each other and do it in a manner that's timely and effective.

Now, I don't know why this slide was put up there. This is Andy's slide for achieving circulation. Here's what I'm thinking. Having been—having served as the NCCIC Director, the NCCIC does, in fact, circulate information amongst everybody, and having everybody with a seat at the table is critically important. And if you think about it, something that may be considered innocuous or "Hey, you know, it only happened to me. It's only my problem" may be part of a broader campaign, and we're certainly seeing that with some activities that both law enforcement and DHS has been dealing with over the last 12 months, where seemingly independent activities, we've been able to link together through NCCIC analysis as part of broader campaigns. And we've been sharing that out through the ISACs and other information sharing partners.

But we need to broaden the foundation, and by doing such, it's better to share information so that you can manage your risk and better harden your defenses, and trust is a critical factor in that. We're opening the Kimono in the NCCIC, so that people can see what information we're getting because, frankly, there's a lot of folks out there who think that the Federal Government is holding back and we've got all sorts of classified information. The NCCIC does operate at the Top Secret SCI level, but all of the partners who are in there—public sector, private sector, and the like—they see everything that we see, and that kind of information sharing helps build trust. Frankly, we're pushing every day to declassify as much as possible. We don't want to build a huge classified infrastructure because that sets up the environment of some folks who can build it because they have the resources. Those are the haves, and everybody else who can't afford that become the have-nots. We're all in this together. So we're working hard to declassify as much as possible, so that we can better share information across a broader community set.

But the NCCIC, you can join the NCCIC today by signing up for our CISCP program, our Cyber Information Sharing and Collaboration Program, or the Enhanced Cybersecurity Services, where we provide our information out to commercial providers who have been certified to do managed front-end services. Wouldn't it be cool to use the same type of information that the

U.S. government gets from all of its different sources and have bad indicators and the like blocked before it even gets to your company or your entity? Yeah, I think it would be cool, and we're already working with a lot of different providers to move forward on that with the Enhanced Cybersecurity Services. So we are moving forward to build a nice, solid foundation upon which the country can move forward.

Now, as I mentioned, I'm an acronym jihadist. I don't like acronyms, but I'm going to try to define every single acronym that I'm going to be using in this briefing. If I don't, I want you or raise your hand and shout out at me and publicly chide me. This is recorded. So I'd like you to shame me if I don't—if I don't define something for you in advance, okay?

And with that, let me show you some folks that we are sharing information with, and this acronym here is STIX and TAXII. Wouldn't it be cool to automatically share machine-to-machine information? You know, right now, we've had a lot of folks that have grown up, getting used to sharing information, and you get information about an event that occurred like in the fall, but that's not necessarily fully helpful. We need to get from months to milliseconds, and that's our goal, is to get from months to milliseconds.

So last year, the Department at the end of a research and development effort launched a prototype of what's called STIX and TAXII for automated information sharing. STIX stands for the Structured Threat Indicator Expression, and that "X" is "Expression." Think of that as the payload, about 28 different attributes about an incident. Now, there's actually about 100 fields, but 28 are the core of the information about an incident. TAXII is the mechanism of getting it to you. Think of it as a protocol like simple mail transport protocol, but we had to have a protocol to get it out to folks. And it's the Trusted Automated Exchange of Indicator Information. Now, frankly, I think that the guys who put together these acronyms made up the acronyms and then filled in the blanks afterwards, but it works. And the prototype was a success. We are now going to full production. We've gone into—from just a dedicated server at one of the MITRE facilities that we had contracted with, we're going into the Web with one of the famous cloud providers, and we're already hooking folks up. And the financial services sector has already commoditized STIX and TAXII into their Soltra Edge product and has been sharing information within the financial services sector.

These are some of the folks that we were partnering up with, but as you take a look at information sharing, getting from months to milliseconds is reliance on automation. And with STIX and TAXII, we've got the capability that is going to help us leapfrog forward in a manner than we are—that the nation needs.

So here's the timelines. You know, it was concept in '13. 2014, yeah, we got into a prototype with a single one. Now in '15, we're on the Web, and we're building it out even more. But what about information sharing through other means? You know, in the past, it's always been the ISACs as our primary entries, Information Sharing and Analysis Centers, taking a look at those 16 critical infrastructures and getting the like entities together, but you know what, we were getting a lot of feedback from folks who weren't considered part of the critical

infrastructure saying, "Well, Greg, how do I get information if I'm not a member of the ISACs and I don't have a good fit with any of the ISACs?" Well, the ISACs have been great partners. Some have invested in having people into the NCCIC, but we were looking beyond just the 16 critical infrastructures.

You know, for example, the American Bar Association has got a bunch of lawyers that have all got a lot of information. If you think about a lawsuit—and I'm not a lawyer, nor do I play one on TV. I'm a geek. But the lawyers were gathering up a lot of technical information, and they were proving to be a very lucrative target for folks, you know, who were engaged in criminal activity, such as industrial espionage, and other folks who were looking to seek aggregation of information.

How were we getting the information out to that information sharing organization? Well, we weren't doing as well as we could, and that's one of the reasons why, under the executive order, we looked to create these Information Sharing and Analysis Organizations, and frankly, I for one look at the ISACs as a subset of ISAOs, the Information Sharing and Analysis organizations. We can't just limit ourselves to certain constructs. We need to share with folks who collectively collaborate and communicate because, like a good neighborhood watch, that's a way to effectively communicate.

So we're collecting best practices, and we're trying to share amongst everybody else, but we were also trying to use those best practices as we build the ISAOs. And as we go out and we have these conversations with you all and others, we were foot stomping: Please sign up today for the CISCP program, the Cyber Information Sharing and Collaboration Program. Consider subscribing for services under the Enhanced Cybersecurity Services Program, and go to the NCCIC and download that information that's out there. And, oh, by the way, for the NCCIC, one of the great sources of information—and there's plenty that are out there, but the NCCIC is trying to accumulate and fuse them all together. A website to remember, http://www.us-cert.gov. I say it again: http://www.us-cert.gov. Operators are standing by. Go visit it today. Call today. Now, I don't remember the number off the top of my head very well, but I believe it's 1-888-282-0870. I double dog-dare you to call it sometime today, and call the NCCIC and just do a phone check. Put it in your cell phone. Make it one of your contact numbers, because I'm from DHS, and I'm obliged to say if you see something, say something, okay?

All right. So CISCP, what do you get from CISCP if you sign up? A lot of folks are saying, "Well, you know, it's another government program. Why should I bother?" Well, here's some of the things that you're going to get, and one of the things, a lot of folks say, "Well, hey, how do I get on a mailing list? How do I get on the list server for your guys?" Well, join the program. Subscribe and you'll get the different products that are out there, such as these type of things. Will this be valuable to you? I hope so. Will it be valuable to chief information security officers and CIOs? I hope so. Can it help buy down the risk that you and your businesses will have? I know so. Consider joining, and help us be a—join me in being a cyber evangelist. Help pass the word. This is a great program.

Also, if you're part of a company somewhere and you're looking at your provider for Internet services, is dollars and cents your only consideration as part of your risk calculus? I submit if it is, then maybe you need to broaden your aperture and take a look at "Am I getting value-added services from my provider?" I would recommend that folks consider including Enhanced Cybersecurity Services as part of their risk calculus and in taking a look at their providers. Am I, in fact, getting some risk management provided by my provider, participating in this program, being able to filter some of those indicators that are already known to be bad and leaving you and your team to manage the things such as behavioral analytics and some of the other things that can help you buy down your risk further?

And then, you know, I already talked about the NCCIC, but we had to throw this up there to prove. The President did come to the NCCIC, which really magnified the fact that this is, in fact, the nation's integration center for the sharing of public and private sector information. As you can tell here, Secretary Johnson is looking at me right now to make sure that I am talking to you and making sure that you understand that we're here to help 24/7 in the NCCIC. We're working for you, and we are looking for you to give us feedback. Help us help you by letting us know what information you want, when you want it, and what format you want it.

Okay. Some of the things that we are distributing through the NCCIC, through that website that I talked to you about, the alerts, the advisories, the bulletins, technical documents, and I mentioned the website, http://www.us-cert.gov. ICS has got a page off of that as well that's focused just for the Industrial Control Systems.

But one of the things I also want to foot stomp—and Secretary Johnson would be upset if we didn't—is the commitment our Department has to privacy, civil rights, and civil liberties. Under the Homeland Security Act of 2002, we have what's called the Protected Critical Infrastructure Information program, PCII, and in essence, this gets back to the neighborhood watch construct. We preserve the anonymity of our sources because your brand and your reputation are critically important, and once that's gone, it's never going to get back into the bottle. And the Congress recognized this in the Homeland Security Act of 2002 and created the program, such that if you come to us at Homeland Security, we're going to treat it with privacy protections to protect your identity and your anonymity. That's why when you take a look at different products that we put out, we're not going to say, "Well, this particular piece of code was associated with the attack on this particular company." We don't do that because we want to continue the information sharing, and that goes both ways. We protect your brand and your reputation.

And our Privacy Office is established under the force of law with our birthright documents. Privacy is built into all of our processes, and last year, we even got an award from the ACLU for our privacy program. And when was the last time the ACLU ever gave and award to a government agency? Go figure. But I'll tell you, it's engrained in what we do. So we want to make sure that we continue to do that and we do regular audits on privacy and the like, and since that law back in 2002, we've never busted trust on privacy.

And with that, PCII, if you come to us under the PCII program, critical information—infrastructure information, you are protected from FOIA disclosure, state and sunshine laws, local laws that pop up. That information is protected from use in regulatory actions and from disclosure and civil litigation, which a lot of folks find very attractive in sharing information with us versus other sources. So basically, we'll take that information for the common good as part of that cyber neighborhood watch. We'll get that out, but we're also going to protect you.

Now, that said, if, in fact, you're controlled under a regulatory regime that does not give you a Get Out of Jail Free card from going to your regulator, you still have to do your regulatory reporting, but for the purposes of cyber information sharing, this has been a fabulous program. And I wanted to foot stomp and make sure that this is available to you.

Now, as we take a look at the nirvana, this is what we want. We want to be a perfect information source for you out of DHS and with our partners in the other departments and agencies, such as law enforcement, intelligence community, and the like. But here's what we're looking for in the perfect partner in the private sector. We're looking for folks who do implement the cybersecurity framework. The fact that you are here today, I believe, is indicative that you are on that path, and you probably are already doing it. We want some—we want partners who are willing to invest in managing their own risk by investing in ECS capabilities. We want partners who when they do detect an incident lets us know about it. We want partners who share information with their peers through Information Sharing and Analysis Organizations. We want information sharing to DHS and peers through our CISCP program. And further, if your resources allow for that automated sharing of information, that you subscribe to STIX and TAXII information sharing products, and that can be within the ISAO, like the financial services sector is already doing with the Soltra Edge product, or other mechanisms such as subscribing directly to DHS for STIX and TAXII products.

So here's what I'm looking for. I'm asking you to help me carry the message into taking a look at your options for STIX and TAXII for your companies' products. I'm looking for you to join the C-Cubed Voluntary Program and implement that Cybersecurity Framework. If you're not already a card-carrying member of CISCP, our guys from our CIKR team, such as Mike and Azzar, you know, they're here to help you get into that. And then learn more about the ECS program, the Enhanced Cybersecurity Services program because I think that's going to be very valuable, and I think in the marketplace, the marketplace is going to clamor more and more for that, and we're already getting stress within our resources to move forward on that, but it's something that I think we need to prioritize as well.

So, folks, that's a quick rundown on what we believe is the future of information sharing from a DHS perspective. At this point, I'd like to open the floor for any questions, comments, queries, or letters to the editor, you may have for me. Are you grabbing the mic? Yes. Okay. It's better—you might have just kept on walking out.

[Laughter.]

CHRIS BLASK: I haven't decided yet, but—so, Greg, Chris Blask with—well, with Webster University Knowledge Center—

Brig Gen GREGORY TOUHILL: My Industrial Control System friend.

CHRIS BLASK: Yes. So we have the ICS ISAC, and the Insurance ISAO now inside Webster, and so just commentating way, I guess I'll do a Jeopardy and phrase this in the form of a question to get your thoughts.

Brig Gen GREGORY TOUHILL: Okay.

CHRIS BLASK: We agree a thousand percent with the executive order, the proliferation of nodes, so sort of interested in your thoughts of how large do you think that scale is, how many ISAOs or sharing organizations, by what definitions do you think we'll end up with in what time frames, or have you thought through that?

Brig Gen GREGORY TOUHILL: I've thought through it, but I'd like to caveat, Chris, and thank you for the question. I'd like to caveat with the beginning. My views on this are not reflective of the Department's, the Pope, or the Commissioner of Major League Baseball. They're mine and mine alone.

I think we may see over 200 different ISAOs pop up over the course of the next 3 years, and they're going to vary in size from organizations. And I mention the American Bar Association as an example. You know, I think that professional organizations that are very well established and very well organized are going to be a rich source of information sharing but maybe not on the scale with the automated information sharing that we've already been fielding, but rather through other mechanisms, such as information sharing that we're putting out through CISCPs and the like. I think what we as the government need to be prepared for is all flavors, and that's one of the strengths of addressing the ISAOs themselves as opposed to staying solely within the bounds of the critical infrastructure buckets that we had previously been focusing on.

Now, that said, the ISACs are continuing to provide great capabilities and the like, but as we take a look at our strategic initiatives to try to get out to everybody, we've got to be prepared to address large, small, and medium businesses as well as the general population. So we've got to be prepared to share with everybody.

SCOTT ALGEIER: Sir, thank you. Scott Algeier with the IT-ISAC. So a question and a comment, potentially. So on the STIX, I guess this is a request for help. Can we get the CISCP team to start sharing STIX files in STIX format? They're sharing it in a format that isn't STIX compliant, and it's making it really difficult for those of us who are trying to consume the information to consume that. So it seems to be some type of proprietary version of STIX that you all are sharing the information in, and it's very difficult for our members to digest. We raised this with the CISCP team, and we'd like some assistance, if you can, to get that sorted out.

Brig Gen GREGORY TOUHILL: Well, thanks. I'll take that on with our team and get back with you. If you would, though, before you leave, would you make sure that Mike gets all your contact information—

SCOTT ALGEIER: Sure.

Brig Gen GREGORY TOUHILL: —so we can get back with you directly?

SCOTT ALGEIER: Sure. Mike knows where I live.

[Laughter.]

Brig Gen GREGORY TOUHILL: Yeah. Okay.

SCOTT ALGEIER: My other comment would be, at least for the IT-ISAC, we share the goal of trying to get information out to more people.

Brig Gen GREGORY TOUHILL: Mm-hmm.

SCOTT ALGEIER: We put proposals together in private to DHS, which has gone nowhere. We'd still like to consider working on those, if we can, at some point. You know, this—there's some concern out there within the ISAC community. At first, we were assured that ISACs would be grandfathered from the ISAOs, and now, of course, we're not. And so there's really a lot of concern out there that what's going on is going to disrupt the organizations that have been out there working on this successfully for 15 years or more, without any regulation, without any—responding to our members' needs. So there's really kind of a concern for many of us out there. You know, again, we're here today. We want to be good partners. We want to contribute, but we've had ideas in the past on how we can achieve the same goals that really haven't gotten—really been responded to by DHS in the past.

Brig Gen GREGORY TOUHILL: Well, I appreciate that feedback, and, you know, frankly, I don't know all of the different struggles that you've had, but I want to be part of the solution for the future. So before I leave, I'll make sure that I give you my card, and then you can—you and I can have a conversation a little bit deeper, so I can dig into this and do a better job for you. How's that?

SCOTT ALGEIER: Very good. Thank you.

Brig Gen GREGORY TOUHILL: Okay, thanks. Any other questions? Comments? Queries?

ATTENDEE: Hi. Just a quick question. You mentioned scaling in terms of small, medium, as well as large-size businesses, and I wonder if you could elaborate a little bit on what you think needs to be done and assess where we are today with regard to some of the outreach in

programs you've got as it concerns small and midsized business and information sharing as well.

Brig Gen GREGORY TOUHILL: Yeah. Thanks very much. Once again, these are my views. You know, as I go around the country and I'm talking cybersecurity best practices, I'm having the conversation with the cyber neighborhood watch. My teams are going out and doing incident response actions. We're talking with private sector companies that are assisting companies with private sector incidents and the like. One of the themes that I personally am seeing is the large companies that are out there largely get it, and they have resources to go and harden up their defenses. They're a bigger target. So I would think that based upon what I'm seeing, the vast majority of the folks that are cyber criminals and crooks and nation state actors are going—when they're going after a private sector entity, the vast majority of them are going after big guys. However, based upon my observations, more and more times, you know, it's the old Willie Sutton argument. Do you remember Willie Sutton? Why do you rob banks? Because it's where the money is. The geek in me goes back to my engineering school days where, you know, it was learn about resistance, and I remember—

God bless you.

I remember my professor talking about resistance, and you take water and then pour it down a display, and the water would flow where the path of least resistance is. The larger companies are investing more and more on cyber defenses. The bad guys still want to go in the Willie Sutton approach. They want to go where the money is. A lot of the large companies are now raising the bar and making it more and more expensive for the bad guys to get into them. So where are the bad guys going now? They're going in the path of least resistance. They're going for the medium and the smalls and with increased frequency, and the days of the small businesses saying, "Hey, I'm too small to be a target," those are long gone.

With automated tools that are out there, I can go on Metasploit. I can do Nessus scanning, and I can go out there and I can find a target set and take advantage of them. We're at the point now—and I think it's—the inflection point already occurred a while ago, where the small and mediums need to be paying attention. They need to have the capability, and that's maybe where managed services come in where folks pool resources. They go to a service provider and the like, and having discussions through information sharing helps raise that bar.

I think small and mediums are under increased risk, perhaps even more so than what they've thought they were in the past, and I think as we take a look at the future, we've got to make sure that we are sharing with everybody. I hope that answers your question.

I think I have time for one more question, but you're standing up like I've got to go? Or no, you've got the microphone. Sir, over to you.

SEAN MOORE: Good morning. I'm Sean Moore with Centripetal Networks.

Brig Gen GREGORY TOUHILL: Hi.

SEAN MOORE: A little new to this space, and I'm curious if the commercial threat intelligence providers, the Inside CyberLenses [ph], emerging threats of the world, are they interested in taking threat intelligence data, repackaging it, and reselling it, or are they allowed to do that?

Brig Gen GREGORY TOUHILL: Oh, I think there's already a marketplace, and thanks, Sean, for that question. We're already seeing a great market place in the information technology business where folks are actually going out there and generating threat intelligence and marketing. I mean, it's a good business model, and we certainly don't want to disparage anybody's business capabilities.

That said, we get—there are many different providers of threat intelligence who, in fact, do share with us, and they package up products that they give to us with the express patriotic interest of making sure that stuff gets out to the general public. And we thank them privately, and they ask us not to thank them publicly. But there is, in fact, a business model out there, and for a lot of companies, we do make recommendations to them, depending on their risk appetite, the type of critical infrastructure environment that they're in and the like, that they do, as part of their risk management construct, invest in a cyber threat intelligence capability, either organically through their own corporate resources or through subscription or even having companies on retainer. Does that answer your question?

SEAN MOORE: Yes, sir. Thank you.

Brig Gen GREGORY TOUHILL: Very good. Thank you. Larry. Yes, sir.

LARRY CLINTON: Thank you. Larry Clinton, Internet Security Alliance. I sometimes think we talk about a lot of different things together, and I want to kind of separate some of these out. So we're really interested, as you said—and I agree with you, 100 percent—in getting more participation from smaller and midsized companies because these are increasingly the vulnerability targets. But the issue seems to me to be not so much to get these people as part of ISAOs as much as to make the information that they get more actionable to them, and for them, there's often a major cost issue here. They simply don't have the economies of scope and scale—

Brig Gen GREGORY TOUHILL: Right.

LARRY CLINTON: —that the larger guys have, and I'm not clear how we're envisioning the ISAO process as addressing that particular need, and a sister problem to that has to do with what we're trying to do here is expand participation, and we're going to come up with the rules for participation through the standards organization. But it seems to me that there's a natural conflict between developing a broad rules set of entities to qualify as being an ISAO, yet potentially liability protection, et cetera, and the ability to be an organization that can meet this expanded rules set. And I'm really not clear what the—what the game plan is for that. I mean,

the more specific we make the rules and requirements to be an ISAO, the fewer ISAOs we're going to get, the fewer participants, et cetera, et cetera. So if you could help me think through some of the thinking on this, I'd really appreciate it.

Brig Gen GREGORY TOUHILL: Well, thanks, Larry. There's a couple of questions in that one, and frankly—and I took some notes here. You can sit down if you'd like.

[Laughter.]

Brig Gen GREGORY TOUHILL: No. Larry is a friend. I just want to make sure he's comfortable, and you can come back to the mic if I don't answer your question. How's that?

A couple of things. First of all, I think those are excellent questions, and I feel like I'm at a disadvantage because I don't have my counsel here by my side because some of it falls into the questions of law and the like, particularly when we talk about some of the liability protections and such. And as Ben mentioned, you know, the Congress is working right now with some information sharing legislation that is going to address the liability protections, and I still have a two-dollar bill on the table that they are, in fact, going to get a bill in front of the President for signature by the end of this month. To bill, tou Hill. It works. Okay.

[Laughter.]

Brig Gen GREGORY TOUHILL: But as we were—as the concept of the information standard—you know, Information Sharing and Analysis Organizations was really congealing. We wanted to pay respect to the ISACs as well, but the ISACs, it was well established. The FS, the financial services ISAC was created back in, what, '99, it was—you know, came into its current form? Is Denise here? I didn't see Denise here. Yep, there's Denise. '99, Denise?

DENISE ANDERSON: '99.

Brig Gen GREGORY TOUHILL: Okay, good. So the Alzheimer's hasn't kicked in yet.

But as we were looking at the model for the broader information sharing organizations, for those who didn't fit with the standard ISACs—you know, ISACs were functionally aligned across the critical identification, which was designated through a previous executive order. 13636?

ATTENDEE: Yeah.

Brig Gen GREGORY TOUHILL: Okay. Hey, I am impressed myself. I even remembered the number on that, and I'm not a lawyer.

So we already had a pretty good definition on the ISACs, but who is an ISAO and who is not an ISAO and who do we share sensitive information with becomes kind of a challenge. So the discussion was, well, let's not play politics with who is in and who's out. Let's go to a standards

organization to actually go out and define it, and then have an independent arbiter of who is an Information Sharing and Analysis Organization, so that we can best and fairly represent everybody's equities.

So that in and of itself within the government bureaucracy process has been a big challenge for guys like Mike Echols and the like in trying to go through with a request for comment period and all the adjudication to go through it, and as everybody already knows from their civics class back from sixth grade to twelfth grade, the United States government is not built to be efficient. It's built to be a fair government. So we're not moving as fast as everybody wants, including us, but we want to make sure that we're being fair and we're being equitable, and that process that we are following with that is just that. We want to make sure that as we are going through that process, it's transparent, it's equitable, and it produces a fair product.

Now, that said, having a standards organization help define what exactly are those criteria for entrance into the club is critically important, and we want that to be transparent, but we also want it to be independent. So that's where we stand on that, and that's why we took the approaches we did. Does that address the question?

LARRY CLINTON: That's really helpful. Thank you.

Brig Gen GREGORY TOUHILL: Okay. Thank you, Larry. I appreciate that question, and it's important to get that out on the table. Thank you.

Are there any other questions before we adjourn for the next session? We have another question. Thank you. And this is the last question, I've been informed. Otherwise, Mike, who is a lot bigger than me, is going to whoop me.

[Laughter.]

CHRIS KREBS: Chris Krebs with Microsoft. Less of a question—

Brig Gen GREGORY TOUHILL: Hi, Chris.

CHRIS KREBS: —and more of a suggestion or an ask. So we've already heard today a lot of conversation about ISAOs. We've heard about ECS. We've heard about CISCP. We've heard about C-Cubed. In thinking back—

Brig Gen GREGORY TOUHILL: A lot of acronyms, huh?

CHRIS KREBS: Right. Well, and then all the executive orders dating back even to the National Security—or National Strategy for Information Sharing.

Brig Gen GREGORY TOUHILL: Mm-hmm.

CHRIS KREBS: So when—as these initiatives proliferate, I reach back into my company to, you know, vector in the appropriate technical expertise to feed the request for comments, to feed into applications, things like that.

Brig Gen GREGORY TOUHILL: Yeah.

CHRIS KREBS: What would be really helpful to me is I make that internal sales pitch to provide some assistance here as an overlay. Like I said, we've got a lot of initiatives, and it's not immediately clear to me where each of these initiatives falls or fits and what the unique value propositions of each might be. So if the Department could provide some sort of overlay of—you know, even a one-pager or two-pager or whatever—of what each of these programs represents, what they're trying to accomplish, the value proposition, and then push that out, that would help companies like Microsoft and I'm sure many, many other companies, and even as organizations contemplate standing up ISAOs, what they can get out of the process and how they can play ball.

Brig Gen GREGORY TOUHILL: Thanks, Chris. That's really helpful feedback, and, you know, we do have them. And perhaps we just haven't done a good enough job getting it out to you and others, but I will tell you what. I'll guarantee you, if you sign up with Azzar and Mike and our team here before you leave today, by the end of the week it will be in your inbox. Is that good?

And special deal for you. I'll be in Seattle tomorrow. I'm willing to come over to Microsoft and brief, if need be, okay? All righty.

Any other questions? I'll be out in the hallway for about a half hour before I have to head back. I am flying out to Seattle for my daughter's graduation, so I've got to get back to Washington and pack. But thank you so much for your kind attention, and thank you for the great questions. We look forward to the greater information sharing for the rest of the day, and thank you for being here. Hope you have a good conference.

[Applause.]

Executive Panel

MIKE ECHOLS: Mr. Matt La Vigna, Director of Operations for the NCTFA—I'm sorry—NCFTA. And then Mr. Sam Visner, Co-Chair of the R&D Task Force.

[Pause.]

MIKE ECHOLS: Thank you very much. So thank you, panelists, for being here. First, I'd like to go to Mr. Riggi to give you an opportunity to make a couple of statements.

JOHN RIGGI: Sure. Thank you, Mike. First of all, I'd like to thank you, Mike, and DHS for graciously inviting myself and the FBI to participate in this very, very important conversation.

Before I begin, can I just have a show of hands, how many folks we have actually from the private sector, nongovernment folks? Good. More than I thought. Excellent.

So somewhat echoing General Touhill's comments about the need for information sharing and the FBI and law enforcement in general, Secret Service and our partners at DHS, we understand that to prevent crime, solve crime, we need the public's assistance, and over the years, to combat, whether it was drug trafficking, trafficking, organized crime, violent crime, even bank fraud, we were very active working with the private sector, financial community, to establish outreach programs and to garner those, as General Touhill mentioned, the cyber-hood—the neighborhood-type watch programs. Well, that was in the physical world, and as General Touhill said, we need the same in the virtual world because those crimes, those acts are occurring on private networks. As you know, they're not occurring on the streets, in the homes, the physical world.

And in the FBI, we have several programs beyond our individual community outreach programs, which are run by our field offices, that strive for that effective community outreach. On a national level, we have what's called the InfraGard program. It's kind of two words combined, "infrastructure" and "guard," but the "guard" is g-a-r-d, and that consists of 36,000 individual members. It's not organizational, organizational based. Bottom line, you just have to be a U.S. citizen and not have any criminal history. You can be a member of InfraGard, and that's spread out through 83 chapters across the United States. Some of those chapters are very active and have developed their own cyber special interest groups along with other special interest groups.

And of course, there's, organically developed over the years, certain cybersecurity information sharing groups that we promote, support, participate in, including the NCFTA, who Maria Vello is here from, National Cyber Training and Forensic Alliance [*sic*]—if I get that correct—but it's a great, great example of the public-private partnership and how we engage directly with private sector academia, and the FBI actually has a full-time unit embedded in that entity. And not only do we have access to our systems, our classified systems there, all our partners there have been given clearances and were able to share and more collaboratively against common cyber threats.

I think you really just—just look at the newspapers during the day, any given day, especially this week, and you will see that the same cyber threat actors that are targeting private sector, such as the health care industry, are targeting U.S. government networks. As you've heard about the major breach at the Office of Personnel Management, you see that it's a shared threat, so it must be a shared defense. So I am very, very excited to be here and be able to participate on behalf of the FBI. Thank you.

MIKE ECHOLS: Thank you. Denise?

DENISE ANDERSON: Thanks, Mike, and thank you for inviting me here to be on this panel. I really appreciate it, and I'm very happy to be here in Boston.

I'm going to give you a little background on the National Council of ISACs. So we were formed in 2003, so we've been around for over 10 years. We were created to actually—as an ISAC community, foster between each other, the challenges and opportunities that we had as a community going forward. So we actually collaborate very heavily with each other. We collaborate on a daily basis between our operations centers. We collaborate on—if there's a crisis, we're on a call collaborating with each other. We have a list server and a portal where we're sharing on the list server over 20 or so items per day between the sectors, and then, of course, we actually have presence on several watch floors where we actually also collaborate, including the NCCIC, the National Cybersecurity and Communications Integration Center. So we have a very strong community where we're constantly interacting with each other.

We also participate in, of course, exercises with DHS in Cyber Storm, and then we have 19 ISACs that are currently members of the National Council of ISACs.

As far as the ISACs themselves are concerned, they're basically communities of trust, and they actually do a lot more than just information sharing, which is a point that, hopefully, bring out here that information sharing is a tool in the tool box to help us mitigate threats.

So we have strong reach into our sectors. We're subject matter experts for our sectors. We have a very strong response capability and collaboration capability in response, so that if—and this is a role that has been carved out in the NIPP, the National Infrastructure Protection Plan, where we actually play a role in response, coordinating on behalf of the critical infrastructure sectors.

When it comes to ISAOs, of course, we are an—you know, we are ISAOs because we do share information, and we do analyze it. And we support the movement. Actually, many of us are actually standing up ISAOs for various sectors that don't fit in neatly into the critical infrastructure. So that is something that's exciting and that we fully support, but we also want to make sure that the ISACs are recognized for their unique capabilities and their roles outside of information sharing.

MIKE ECHOLS: Thank you. Sir.

RICHARD SERINO: Good morning.

MIKE ECHOLS: How are you?

RICHARD SERINO: Good. I'm Rich Serino. I'm currently at Harvard and not MIT, so I'm actually not sure why I am here. I did spend about 5 years in Washington as a Deputy Administrator at FEMA, and when I say I'm not 100 percent sure why I'm here, I'm honestly saying that because there's a lot of talking about the ISAOs and the ISACs and every other acronym, and when I was

at FEMA, I was involved in a lot of those. But I'm actually going to stray from that a bit and talk about what—the importance it is to have the private sector and government work together. At FEMA, I had the opportunity to help develop something we called "whole community" that a lot of people have heard, and an offshoot of that turned into "whole of government"—and how we were able to bring people together. And I won't dive in depth into all of them, but quickly, it's government at the federal, state, local level, but then also how we're able to bring together the nonprofit agencies, the Red Cross, et cetera, the faith-based community, and the private sector.

And prior to 2009, we did not have agreements with the Red Cross. We didn't have agreements with the faith-based community, and we certainly didn't have, working with the private sector. But what we did is brought them in and to be part of the team. In 2010, during the Haiti response, initially, I was in the National Response Coordination Center, their country's emergency operations center, if you will, and in there, as Haiti is happening, I turned to our director of response and said, "Where's the private sector?" and he said, "They're not allowed to be here in the room." And that to me was rather shocking.

If you haven't picked up—I mean, I am from Boston, born and raised in Dorchester, and I was Chief of EMS across the river in Boston for—I was there for 36 years before I went to D.C. But during the period of time when the private sector wasn't there, we had them in Boston quite a bit in our EOC, all the time, 25-year relationships with Boston Properties, with the Hancock. And so when I got to D.C., I was sort of shocked that they weren't part of it.

So we started, went through a process. Our lawyers told us, "You can't do that. We can't have the private sector in the room." So during a response is not the time to debate that. So about 6 weeks later, we actually looked, and after a bit of discussion, we got a new chief counsel, and it makes things much easier.

[Laughter.]

RICHARD SERINO: And we have about—had—we have about 200 lawyers are FEMA and had someone who got to "Yes" and figured a way that we had private sector representatives in the National Response Coordination Center within 3 months, and we had that, developing the team, and then from that, we built the ability to have them in there for 3 months at a time. We had started with Target and then Citibank and all the different sectors.

In an outreach of that for a year later, we had something developed called the NBEOC, the National Business Emergency Operations Center, and during a crisis, that was stood up. And there were over 500-plus companies that can be part of that, that they actually will share information that make a difference in people's lives during an emergency. It's whether it's able to have Wal-Mart send water or food, whether it's smaller companies to understand what's going on and how they can help protect themselves during whether it's Super Storm Sandy, whether it's during tornadoes, during whatever the emergency is. So it really helps make a difference.

And now that I've been at Harvard for just under a year now—and at Harvard, with NPLI, the National Preparedness Leadership Initiative, we actually looked at the response to the Boston Marathon bombing, and fortunately or unfortunately, in my role as the Deputy Administrator, I was actually in Boston at the marathon that day after having been the incident commander for the marathon for many years. In looking at the leadership response to that, it actually struck, listening to the earlier speakers, that the response to that was done very well, and you ask who was in charge at that event. And the answer was, if you talk to the governor, talk to the mayor, you talk to the head of the FBI at the time, who was the special agent in charge—you talk to Ed Davis, the police commissioner—not going to say any one person was in charge. It was a shared network of folks, and it was shared because people trusted each other, people had relationships with each other, people had a common sense of mission, and there was no ego and no blame during that period of time for the response during the week. And hearing those four things that the people who studied it came up with very much fit with almost the four things that people mentioned here today: that you need to have trust, a common message, doing this for the common good, and understanding that having those relationships in a crisis truly will make a difference.

I'll stop there.

MIKE ECHOLS: All right. So there should be no question why you're here now. That's exactly the message that we're trying to promote.

MATT La VIGNA: Hello. My name is Matt La Vigna. I'm the Director of Operations for the NCFTA, the National Cyber-Forensics and Training Alliance. Before I get into that acronym, I'll give you a little bit of background on myself. I come from—I had a couple different perspectives on information sharing, one from an agency standpoint, a government agency standpoint. I recently retired from the Secret Service, and with our electronic crimes task forces and our community outreach, just like other law enforcement agencies, whether it's state, local, or federal outreaches, it is extremely important. And some of the differences at a local level are most people will know each other as opposed to a national-level outreach, and so I've seen it from a headquarters perspective where most of the time, you're feeding information out to people, and it's a one-way channel.

At a local level or, say, on a regional level, it's a little bit better, so it's kind of like Information Sharing Lite. You get members. You sign them up. They get into your group. You give them some information. You have some meetings. You encourage them to communicate, but it's really—a lot of times, it's hit or miss. Different initiatives are more robust than others.

And now I'm at an entity that I would say is an Information Sharing Plus or information sharing on steroids. The National Cyber-Forensics Training Alliance was created back in 2002, and the issue that was—it was created by thoughts of agents from the FBI and private industry. The issue at the time was industry sharing information with government or law enforcement was good, but it immediately became classified and virtually impossible or difficult to share with

anyone. So it was—there, it's one way. It's coming in, but it can't go out, very frustrating. So you have the—in Pittsburgh, you have the FBI's High-Tech Crime Task Force working with other law enforcement, which is great. You're in a task force environment. Everything flows. You're good. But in a law enforcement task force environment, you don't have industry sitting in there. So think of office space, and you're in a federal agency, and everything there is classified. And so getting private industry in there is very difficult. How many months does it take to get a clearance? How many times are you going to do that? How much does that cost?

So the idea came up: Let's find this neutral ground in order to share information in an unclassified environment where we don't have the restrictions of the government space. We can't go to private space. The government can't occupy the space. You know, bank can't host law enforcement's office space. We can't go down that road, but we find neutral territory, and that's where the NCFTA was formed, so back in 2002.

When it was created, it was—and it still is—a clearinghouse or a safe harbor for sharing information, so personally and physically sharing information. In-house, we have federal law enforcement agencies, an entire FBI unit that is embedded there in our office space. Secret Service is there. Homeland Security Investigations is there, Customs and Border Protection, U.S. Postal Service, the National Crime Agency out of the UK, Australian Federal Police. So we have as big a perspective from a law enforcement standpoint as we can, and then we also have embedded private industry. And so we're able to share information at a personal level with those that are on-site, but then those that are also off-site.

We achieve our goals by facilitating the sharing and aggregating it across different industries and sectors, so it's not just sector-specific. We're able to share that information across the different sectors and across law enforcement. Believe it or not, government agencies and law enforcement don't always talk to each other, and the reality of it is that government agencies are in competition with each other. Sometimes their lanes will overlap. A lot of times, their lanes will overlap, and there needs to be that de-confliction. There's plenty—to be honest with you, there's plenty—we all know there's plenty of work for everybody out there. So all we really need to do is find a way to de-conflict, stay in our lanes, work with each other when we can and when we need to, while serving the needs of private industry.

There's a lot of things that have already been discussed, and I know we're going to talk about a lot of things like trust and facilitating the sharing of that information, but one of the things that's critical is just being a member of, say, an organization is not the end because—I call them a "Looky Lou." You're just going to look and read, and you're just going to absorb this, but it's the two-way sharing that's really important. Trust is what builds that two-way sharing capability, but it's the two-way sharing that is really critical in order to make any of this work.

And so I'll leave it there. I know I usually will keep going if you let me, so—

MIKE ECHOLS: Sam?

SAMUEL VISNER: Thanks. I'm Sam Visner. I'm actually here in—and although I run a cyber P&L for a company called ICF, I'm here representing the Intelligence and National Security Alliance for whom I'm co-chairing the Cyber R&D Task Force, which is working on both trying to strengthen a national cyber R&D strategy and build a national cyber R&D ISAO.

And by the way, as we were all sitting down here, Matt, as we were trying to figure out how we would get all of us at the table, he said we're going to need a bigger boat. I saw that movie recently. I think what they really needed was a smaller shark.

[Laughter.]

SAMUEL VISNER: But they didn't get either. It ended badly for most of them.

What I really am hoping to talk about today is what we will do to improve information sharing for cyber R&D. So first, the why of it, and the why, I think is that while I agree absolutely with Deputy Assistant Secretary Touhill that there is a huge risk component to the cybersecurity problem, I think there is also a larger component that relates to our nation's global role, global standing, and global power. Other countries are using their ability to impair our cybersecurity, to conduct exploitation and attack, to change the global order, to diminish our global role, our global standing, and enhance their own. They look at cybersecurity as the security of bordered sovereign cyberspace in which they intend to become preeminent, and they're pretty clear about their objectives there.

We see more and more complex cyber operations representing the intersection of advanced cybersecurity technology plus really patient, disciplined, effective, well-resourced trade craft on behalf of state actors and organized cyber criminals. So that interaction of great trade craft and great technology in the hands of adversaries, cyber criminals, and state organizations is more than—it goes beyond public safety, and it goes beyond risk. It goes to the very—to our nation's very standing in the global order and our role in preserving both national security and international security. So that's what I really think is at stake here, and that's why I think this issue is critically important.

That's why when we talk about cybersecurity information sharing for R&D, I look back to other issues, other problems, and, Mike, challenged me to be robust in my comments. So hopefully, I will rise, Mike, to that challenge.

But when I think about other problems in which our global standing and global role was at stake, nuclear energy, aerospace science and engineering, which allowed us to become preeminent in aerospace and eventually get to the Moon, these were areas in which we built national strategies for R&D, for nuclear science, for aerospace science. And having built those strategies, we started to build real information sharing architectures in the post-war era, and then eventually, we began to build information sharing, not only information sharing architectures, but organizations.

And so my contention and the contention of those with whom I'm working in the Intelligence and National Security Alliance, that if we're going to be effective in cybersecurity, we need a national cyber R&D strategy to be able to deal with problems like securing critical infrastructure and SCADA systems and industrial control systems and highly virtualized systems and systems that run where workloads are allocated to different cloud environments, which expend—systems that extend all the way from your mobile device all the way through the shop floor on a shared infrastructure and possibly a virtualized and cloud infrastructure. We need to be able to do that, and we need to be able to do that if we are going to preserve our global role. And that means building up some kind of an information sharing organization for cyber R&D.

So the "what" of it, I think is the future of our country, not just our safety, which is important, not just mitigating risk and buying it down, which his vital, but going beyond that to preserving our role on the global order. And the "what" of it is building up the strategy, which I think OSDP is charged with doing, but probably I wouldn't say the results there have been as robust as we need—going from a strategy to an information sharing architecture and a real Information Sharing and Analysis Organization that gives us in cyber what we got out of nuclear energy, what we got out of aerospace, what we're getting in some areas of biotech, but we now need in cybersecurity for our own national interests.

Let me stop there. I think I've gone on far enough, and clearly, we're not going to get a smaller shark out of this, so we really do need a stronger boat.

MIKE ECHOLS: Great. So we have a very opinionated and learned panel, and so I'm really interested in hearing your insights on some of these subjects. As you can see, we're trying to stretch the subject here so that we don't miss an opportunity when we get in these workshops later, and we don't want to paint ourselves in a corner. We want to think broad. We want to understand those things we need to be considering as we stand up a standards organization and we start looking to best practices and how we roll out an ISAO paradigm that takes us to the level that we need to be at for cyber protection going forward.

Sir, Mr. Riggi, your teams are out all over the country talking to people. You get to see the inside after an event. From a law enforcement and national security perspective, why is information sharing that important pre and post incident?

JOHN RIGGI: So pre incident—and as was repeated here over and over—really the primary function is to establish that trust. I can't say enough how important having that preexisting trusted relationship with law enforcement, whether it's the FBI—or government in general, having that person you know in that government entity that you can call during an incident. Obviously, the other benefits are that when there's robust exchange, you do have the ability to prevent, identity, and disrupt, perhaps, threats that exist, and as we often find, that government, whether it's law enforcement, FBI, or the intelligence services, the national security such as NSA, CIA—we may have pieces of the puzzle of that cyber threat puzzle, but often it's the private sector that has the remaining pieces of that puzzle, those clues and evidence that help us when we combine our information intelligence, help us form a picture of

the adversary, what their intent and capability actually is. Again, this is unlike any other threat that the government has faced, that the nation has faced, where the majority of the activity is occurring on private networks, and contrary to what Eric Snowden has misled the American public to believe, the government does not see that traffic. Over 80 percent of the networks are in private hands. As I said, the intelligence and evidence lies on your network, and we have to combine that information.

The fact that the section I run in Cyber Division exists, it's an outreach section. It's the only operational division, Cyber Division in the FBI that has a permanent dedicated outreach section because we understand the value of the private sector information, and we have moved progressively—and I would say rapidly—to declassify information when necessary and push that out to the private sector. We understand that to defend private networks is to defend the nation.

I think I'll give a little bit of an opinion here also. So post incident, you need to know who to call. You need to have that trusted relationship, and then there's all types of local- and national-level resources that the government, DHS, Secret Service can leverage and be able to respond and help that entity.

Post incident—well, let me get that. One sec. So post incident, we understood that for the private sector to call, whether it's the FBI or government in general, that they need assurances from us that they will not be treated as someone who has caused harm to themselves. They need to be treated as a victim, a victim of crime, and that is in fact how we treat victim companies. When we do respond to an incident now, not only do we send our trained investigations, our computer scientists, but we send outreach specialists. We send victim witness specialists. Often these major companies have had their employees' personally identifiable information compromised. They have to deal with reporting to their local police departments. We help them through that process. We also deploy internal and external communications specialists in helping the company message this out. We say this often, but we are not regulators, on the law enforcement side, whether it's FBI or Secret Service, and we don't call the regulators. We leave that decision to the companies, their attorneys, and the regulators to understand what their reporting requirement is. So we treat the company like a victim of crime. That engenders the cooperation and trust.

Going back to the FOIA Act regarding the creation of the ISAOs, I think the challenge will be for the group, how do you create an ISAO without creating another layer of bureaucracy which may inhibit those direct personal relationships that we need with companies? So that's a collective challenge, I think, just as the challenge is to defeat the cyber threat. You know, I've heard the expression from Mr. Serino today about it's a whole-of-government approach. I'd like to even expand that and say, look, this has to be a whole-of-nation approach. It has to be private sector combined with government. Thanks.

MIKE ECHOLS: So let me go right to you, Rich, then. All of these challenges that we're talking about, all the comments that I receive, they may be related to cyber threat indicators, but

they're the same challenges that I heard about information sharing over the last 15 years, right? So what are some of those best practices? What are some of those challenges, and how did you guys get over them as you form this information sharing?

And if you guys didn't know, Rich helped build the emergency management for Boston. He was integral at FEMA in building some innovative programs to share information and to get better data.

RICHARD SERINO: Well, thanks, and, you know, it's a little interesting now after 40 years of saying "I'm from the government and I'm here to help" that it's—sometimes people say that jokingly, but quite often they are. But the best way to help and the way that we did it was actually something perhaps unique, was listening, actually going out and listening to people and then listening to what they said and taking action after that. And I think that that's really important to do, whether you're dealing with a disaster that's happening, but preferably you've done that beforehand, you've gone out and built the relationships as you're starting to do now and have been doing for a while, is build the relationships with the people that matter, with the people that matter, is something that we changed the word from calling people "victims" to calling people "survivors." And we did that very consciously to change how people view themselves. If somebody is a victim of a disaster or a victim of a cyber event or a victim of a car crash, that presents it in a certain way. We consciously changed that to calling people "survivors," that if you're a survivor of an incident, whether it's a flood, tornado, a fire, whatever it is, you have a much different view in how you view yourself and how the public views you.

And that led us to going down and looking at the whole of community, how we bring a lot of different people together, but I think the most important part is to listen to what people have to say. I spent in every region, in mostly every major city over 5 years, talking to people in small groups, talking to survivors after disasters, talk to people before disasters, to build that trust, to build those relationships.

And for folks in the room and folks who are listening, I think one thing that's important is to make your voices heard, and if Mike doesn't listen to you, go to the next level, and if the Deputy Assistant Secretary doesn't listen to you, go to the Assistant Secretary. And if the Assistant Secretary doesn't listen to you, go to the Under Secretary. That's where I was. I listened to a lot of folks, and believe it or not—I know this may be a shock to you—with every level that I mentioned, their information gets filtered. I know that may be a shock.

[Laughter.]

RICHARD SERINO: But trust me. Unless those individuals make an effort to go out and listen or you don't reach out to them, they may not hear it. I can guarantee you that some direct correspondence to an Assistant Secretary, Under Secretary, maybe even the Deputy Secretary—it took me a while to figure out the chain there, but getting to them will make a difference. Make your voices heard, and assume that the next level up filtered what you said.

So take the opportunity to continue to get your message out, and make sure your voices are heard because that's what will change it. That's what it's going to take for participation.

MIKE ECHOLS: Thank you, sir. So, Denise, we know that ISACs or ISAOs—I'm going to get you all T-shirts to say that, but ISACs or ISAOs. With that being said, ISACs have existed—you guys have been doing this for a long time. What is the difference between an ISAC and an ISAO really, in your perspective and in the perspective of your members?

DENISE ANDERSON: Okay. So an ISAC and ISAO—and actually, I want to, if I can, circle back—

MIKE ECHOLS: Sure.

DENISE ANDERSON: —to some success that we've had as ISACs. The majority of the ISACs have been around for over 10 years. So as was mentioned earlier, FS-ISAC, who I work for, was formed in 1999. Many of us have been around actually 16 years and been very successful, and I think it becomes very clear when you talk to each of the ISACs that they are meeting the needs of the members of that community that they serve.

But where we—you know, we do information sharing, and we do do it fairly well in many cases, and I'm going to point to a couple examples in a minute to answer back to some success stories. But the ISACs also do much more than information sharing, and then again, what is information sharing? It's not just indicators of compromise, as many might think, but it's also sharing best practices. It's sharing lessons learned. It's asking questions of each other about how you're doing things and how things work, and that's what we see with our members. They're not just sharing indicators of compromise, an MD5 hash or some kind of IP address or anything like that. They're also sharing much more than that. And they truly are communities. So what we also do is we're charged with incident response.

The other thing we also look at is we're not just cyber. We're all hazards, so we're looking at physical and well as cyber. And I mentioned the NCCIC, but we also participate in the National Infrastructure Coordinating Center, and we have a role there. We have a seat there on the floor, which actually is pretty revolutionary, I would like to say. I'm coming from the private sector side. I'm saying it on the part of government. We used to have a seat actually at special facility where you had to have a clearance and go in, and we would go in there representing all of the critical infrastructure, not just our sectors, because we wore our National Council of ISACs hat on. But we came to an idea. One of us had an idea, "I'm going to approach the Assistant Secretary of Infrastructure Protection and say, 'Hey, we have one of our ISAC operating centers here nearby. Can we not just have representatives from the NCCIC come to us and we all work together in the room?'" And she said, "That's a great idea," and supported it, and so now we have that in place, and we've drilled it.

So we have a response mechanism where all the ISACs come together. Whether it's a cyber or a physical incident, we're coming together. We're saying, "Here's the capabilities that we can bring to the table. Here are our needs as sectors, and how can we help each other?"

For example, one of the things that we did during—this is not a cyber incident, but it does use transactional data. During Hurricane Sandy, one of the things that we've operationalized as the FS-ISAC is we are able to take credit card transaction data and use that to make sense of certain things. So during Sandy, if you recall, fuel was needed, and there were many gas stations that didn't have electricity. There was people, just boots on the ground, could not respond. What we did was we took credit card transaction data that was actually transaction-at-the-pump data, and we could take that. We supplied it to the NCCIC. The DHS then mapped it out geospatially, so that they could show what gas stations were actually operating and were actually pumping gas, so boots on the ground had that, and that got huge use and recognition across. So that's one of the ways that we can bring those capabilities to bear.

To circle back on the success-in-sharing side of things, because I think we've done it pretty well for a long time, I'm going to point to the FS-ISAC, and when we had the DDoS attacks of 2012, 2013 that affected the financial institutions, we—I like to say our members opened the kimono to each other, but in the case of the DDoS attacks, they not only opened the kimono, they gave each other massages. And the sharing that happened was just incredible.

[Laughter.]

DENISE ANDERSON: I know it makes them uncomfortable when I say that.

The sharing that happened was very—was just amazing, phenomenal, and incredible, and what we did was we had a select group, those institutions that were being attacked, and they were sharing real-time information with each other. We actually were sharing real time within the NCCIC, so government got all of our individual as well, anonymized, so that's the beauty of an ISAC. We can anonymize and aggregate and give the sector perspective.

And basically, we also had a window into some of the bots, so we had a 15-minute heads-up when an institution was about to be attacked, and so you would say, "Heads up, Europe. Bank A, you're about to be attacked." And there were a lot of lessons learned from that, not just necessarily technical lessons, but a lot of best practices that came out of that. But basically, there's three things, I think, with information sharing. It's value, it's trust, and it's infrastructure, to provide the information.

And just as an example of information sharing at its finest, we had an institution—so what we did was we took that small group that was being attacked. We took the information, aggregated it, and pushed it out to the rest of the sector and also other sectors and our government partners. And the last day of the last phase, there was an institution that had not been attacked before that was attacked and had virtually no impact, and so I went back to them afterwards and said, "How was it that you were able to have no impact?" and they said it was because of all the information that was shared beforehand, all the best practices, all the IOCs, everything that had been put in place. They took it. They put it in their infrastructure.

They were able to mitigate, and they had virtually no impact. I think that says it finer than any other thing.

MIKE ECHOLS: Thank you. Sam, you talked about the cyber R&D strategy, okay? So if we could progress science for information sharing the way that we did after, say, the Second World War with nuclear, what would that look like?

SAMUEL VISNER: Well, I think the existing ISACs are largely based on specific industries, but the new executive order talks about moving beyond industries into functional areas. So we're going to setting a precedent here. This will be a different kind of information sharing organization for cybersecurity.

I think, Mike, we've got to do a couple of things first. We've got to define who is going to be in the cybersecurity R&D community, and if I go again back to historical precedent, because we're trying to set a new precedent here, I think of who was the nuclear energy R&D community in the '40s and '50s, key government agencies, key industrial partners. FFRDCs were stood up for some of this work. The National Laboratories were stood up, key universities—MIT; Harvard; Columbia; University of Chicago, where Stagg Field, where the first self-sustaining nuclear reaction took place. So the first thing that had to be done was to establish who would comprise that community, and I would submit that we haven't really done that yet. We need to.

The next thing that I think ought to be done, Mike, is we're going to have to establish a list of the key R&D problems we need to address. Cybersecurity is a huge field, but we're not going to do everything at once at the same speed, nor would that necessarily be wise. So after having established who comprises this community, we're going to have to establish something of a list of key problems that are going to need to be solved. For example, I'm going to speaking next week at a NATO cyber conference in Istanbul about the problem of detecting and characterizing cyber weapons tests because we're not absolutely clear that we know when tests are taking place and when somebody is trying to figure out how effective their weapons are, what our response might be. And if we're going to deter cyber attacks, we need to be able to detect them, and if we're going to detect them, it would be useful to detect the development of those weapons. We don't know how to do that. That might be a key problem.

As we move to the next generation of critical infrastructure in this country—and Smart Grid, Smart Roadways—I live in Washington. We have a long way to go before that gets very smart, I can tell you. But we're going to need to understand some of the key issues related to securing the big data analysis that makes that work. That might be a problem. Smarter people, people who are much smarter than I am are going to have to establish—are going to have to establish that list.

And then finally, the information sharing organization probably ought to play a role in maybe helping allocate effort against those key problems so that not only do we know who comprises the community and what are some of the key problems in order that they might solve, but something about the role that Microsoft might play or the University of Wisconsin might play or

DHS's cyber R&D under Doug Maughan might play, and begin to allocate some of those problems along with some of the milestones. And I think that the goals that we set for information sharing in cyber R&D can't be one bit less comprehensive and ambitious than that, and I think that's the direction in which we need to come.

MIKE ECHOLS: Thank you. So, Matt—and you get the last word here, as time permits—for all the comments that I've heard, for all of the submissions that I receive and the ideas that people have, a lot of them surround things that you guys have already overcome. This idea of having foreign entities and law enforcement and private sector in the same room sharing information, how have you gotten over those challenges, and how does that all work?

MATT La VIGNA: Well, from back in the beginning, it as overcoming that classified environment, and then once you did that, it's building trust. So we've heard that. We've only just started today, and we've heard that how many times? That's got to be the capital-letter word of today, building the trust. You build the trust by establishing those personal relationships and then walking the walk. So what you say you're going to do, you do. You don't break that trust, number one, and you act on the information that you receive.

In the trust, obviously, somebody is going to join an organization and "Hey, we think you should join our organization. Here is what we're going to do," blah, blah, blah. Okay. Sign me up. But initially, they're not going to openly share information. They don't know what it's about. They want to take a look first, "Let's see what's going on," and see results. So is there information coming back to me? So they are going to—and this is just the human factor. They are going to see is there something of value here and am I getting anything out of this. Do I see something coming back? Well, what's coming back is not necessarily—and what we've done is—not necessarily coming back from us. It's coming back from other partners, other members. They are sharing the information amongst themselves, "Here is what we see. Here is what we did about it. Does anybody else see this? Is anybody else affected by this?" Now, that could be within a certain communication channel, but by having the human factor again conduct the analysis—so you have the information sharing and then the analysis on top of that information that's being shared—you're able to cross that from different communication channels, different subsets, sub-organizations, working groups, focus groups, what have you. The analysts that do the work have to be able to see across all of those sectors to know that this information that came from one is similar, same, or affects information in another, and then those correlations have to be put together and then pushed back out. Obviously, it's in a timely manner. We hear back from industry all the time that it has to be timely. If it's not timely, it's just not information. The incident is over. It's gone. "I missed it. Thanks for sharing, but it's too late."

The other thing is that it has to have context around it. So when you are sharing information, the analysis puts context around the information that was received, not just "I'm getting hit by these IPs," or I'm getting his by this or this is happening. It's "Give me some context," and again, this is what we hear from industry, is "Give me context around what you're telling me." And so that's critical.

So it's earning the trust. I think over the years, what has happened is it's earned the trust. I can say that from a government side—so obviously, we have industry, and we have government, cat sleeping with dogs in one place here. The government side, it was only the FBI when it started, so that's just one agency. If we had one agency and one industry, we're not really doing too much, but over time, the trust was built amongst the law enforcement agencies that are there. That was 2002. Now it's 2015. Secret Service just embedded last year, 2014. That took 12 years. So it does take time. The relationships were there. I can say the trust was there at a local level, so we built that trust up. Before that, there were multiple law enforcement agencies that joined, and it was building that trust that was just critical.

MIKE ECHOLS: So this brings our panel to a conclusion, but I want to give Mr. Riggi the last word here, our FBI partner.

JOHN RIGGI: I appreciate that. First of all—well, let me just say, I forgot to mention, I am from Boston, but when the FBI sent me to Birmingham, Alabama, 27 years ago, I started to pronounce my r's, but—quickly.

[Laughter.]

JOHN RIGGI: Again, the themes here, echoed here today, wholeheartedly agree. It absolutely needs whole of government, whole of nation. The discussion, we need to hear from the private sector. Be critical of how the government interacts with you. Tell us what we're doing wrong. Tell us what you need. Be aggressive on your request for information. We do have a saying here in our section, "Share till it hurts," which goes against many of our operational components, but understanding we learned—we the government learned after 9/11 that the emphasis must be on preventing harm, and we learned after 9/11, you just declassify information and push it to the public, to the private sector, who are truly your partners, to help prevent harm, national security harm, public and safety harm, and economic security. That is the way. Even we learned how to take declassified information in the government, downgrade it, push it out, or create unclassified information for prosecution purposes. So we understand it must be emphasis, must be placed on preventing harm, and that's where we'll need to engage with the private sector to do that collectively. Thank you.

MIKE ECHOLS: Thank you. Than you, panel. Appreciate it.

[Applause.]

Advanced Cyber Security Services (ACSC)

MIKE ECHOLS: All right. Next, representing ACSC, we want to bring Mr. Mick Costa to the stage. Mick is the Assistant Vice President of Network Security Services at the Federal Bank of Boston. In this role, Mick is responsible for protecting networks against cyber threats across the entire Federal Reserve system. Mick?

[Pause.]

MICK COSTA: So good morning. So I am Mick Costa from the Federal Reserve Bank of Boston, and as was mentioned, I'm responsible for network security across the 12 districts of the Federal Reserve. The Federal Reserve is not government, except for the Board of Governors in D.C. with Janet Yellen, but the rest of us are dot-orgs, and we're sort of this quasi-government organization.

I'm here today to talk about the Advanced Cyber Security Center. Again, it is one model of cyber threat sharing of an ISAO, I guess you would call us, and I really want to talk about sort of this model—there are a lot of models of sharing—and a little bit about what the ACSC is all about.

So it's a—I guess we'd call ACSC a national model. It's cross-sector, and I'll talk a little bit about that. And it's focused on New England and primarily within Massachusetts. So we are a regional organization and really there to support information sharing amongst other activities.

So there are three areas that the ACSC is associated with. One is information sharing, which is really about, I guess you would say, most relevant to the ISAO conversation in terms of how we share cyber threat intelligence; R&D and education, about promoting research and development, working with universities to bring up a cybersecurity workforce; and then policy development, again, how do we promote good government policies to help support information sharing, cyber threat sharing. It is a nonprofit consortium supported by the Mass Insight Global partnership. Again, it's a Massachusetts-based organization.

So the ACSC and what I am going to talk about today is really about information sharing. The other areas, even though they are parts of the ACSC, I am really here to talk about cyber threat sharing and the initiatives there.

So I was thinking, as I was putting these slides together, how do you carve up cyber threat sharing, information sharing in these areas, and there's a lot of ways to slice and dice it. And I wanted to talk about sort of the context of what the ACSC does amongst other kinds of threat-sharing models. I guess one model I was thinking about is sort of the producer-consumer model. So you have an organization that produces cyber threat intelligence. They produce the information. They are the clearinghouse, and they provide it to consumers. Now, consumers might be people who pay for the product or just participants in cyber threat sharing, but they really get the information from their producer. It's a one-way flow of information.

Another model that I was thinking about is producer—I guess redistributor, and again, I'm just making up these terms; I'm sure there's plenty around—where you have, again, an organization that produces cyber threat intelligence, again, gets that information from whatever sources it can, but it also has a set of consumers that are also producers. So I think about these organizations or these companies that do gather cyber threat intelligence. They delivered it to their consumers, but they are also looking to the consumers to bring information back to them.

So either they are reporting back on incidents. Maybe they have sensors that have been delivered to them that are collecting information about them. So it's a two-way—you know, it's a two-way path of information where the producer is also a redistributor of information, usually anonymizing it and giving it back to the consumers.

Third, I was thinking about sort of the facilitator redistributor, so where you have sort of an organization that does not produce its own cyber threat intelligence. It doesn't collect the intelligence. It's not the place that is generating intelligence information. It's is really providing more of a facilitator role with the consumers and producers. So you think about organizations that are participating. They have threat intelligence, and they are going to share that threat intelligence. They work with a facilitator to facilitate those discussions and those interactions amongst each other and also help to redistribute that information back to the consumers.

Next is the, I guess, purely facilitator role, which his really organizational. So you have the consumers and the producers sharing information. The facilitator really plays a role in terms of just making sure that they are communicating with each other, sort of provides that—just a pure facilitator role, but not a redistributor.

And then last, I was thinking about peer to peer, and I have been in security, in the security area for many, many years. And that was the first model that I actually participated in. It was a group of organizations, different organizations, different CEOs, different structures, and we sat around a table a few times a year to talk about our security programs, to talk about what we were doing, and it was purely face-to-face, physical, with no NDAs in place, nothing in place except for the fact that we trusted each other, that we were going to talk about what we were doing, and trusted each other that we would not divulge or use that for any nefarious purposes.

So I think about the ACSC, I would say we're pretty much in this facilitator, redistributor role. So the Advanced Cyber Security Center itself does not produce cyber threat intelligence information. It doesn't have its own sensors. It doesn't go out to different place to go collect the cyber thread information. It really is partnering with the consumers and producers to collect that information from them, to share that information, and help redistribute it amongst the different participants. So that's really where the ACSC, I guess, would fit within this set of models, and again, there are plenty of these kinds of models out there. We can talk about how participates, the makeup of the participants, the scope in terms of geography or reach or different sectors, lots of different ways of slicing and dicing it, but I thought from an ACSC standpoint, it would be good to talk about just sort of how we interact.

Now, as part of the Federal Reserve, you would consider us as one of the consumers and producers, and each organization that participates is also in that role to different degrees. And I'll talk about that in a little bit.

So the Advanced Cyber Security Center—so we talked about sectors. We talk about participation. We talk about who does what. So here's how the ACSC works. One, it's cross-

sector, so there's multiple industries. It's financial. There's technology industries. There's health care industries, governments, sort of this pure government organizations, and FFRDC. So MITRE is definitely a primary participant and organizer within the ACSC, and in fact, what we do is we have meetings twice a month. So every 2 weeks, there's an ACSC face-to-face meeting. It's held at MITRE on one week and held at the Federal Reserve in Boston 2 weeks afterwards, and actually, there's one occurring this morning that I would normally be at if I wasn't here.

The participating organizations are primarily within Massachusetts, and the biggest reason for that is—we talk about trust. We talk about information sharing. We talk about having a dialogue. These are facilitated by the ACSC, these meetings. I'm a chair of the meetings. There are other people who share those responsibilities too. And they're face to face. We sit down across a table with all of these organizations participating, and we share information. We share information about what we call threat landscape presentations. So threat landscape presentations are presentations that organizations will give about incidents, about indicators, about TPPs, about basically the kind of things that we've seen. And the good thing about this kind of dialogue is that the information is real. So if we think about getting a deluge of information that you can get from lots of places, these are things that have been—this is usually information that's been vetted. It's been seen. We talk about which indicators are actually finding these actions and which indicators aren't, so what's really working, what's not working.

We also have discussions about our programs, our projects, our approaches. So we talk about how we do risk management, the kind of products we're using, the kind of architectures we're talking about, the designs we're using, what's working, right? Because we all have security programs. We're all making investments. This is big money we're spending. What's working? What really are people doing? What are they thinking about? Sometimes it's throwing spaghetti at the wall. It's saying, "We're looking at going down this path. Is anybody else thinking about doing these things?"

We also bring external parties into these conversations. We've had presentations from commercial vendors, from other organizations, from government. People will come in that are invited to come in to talk about what they're doing, what their approaches are, and it's good for all of us to hear those things, and then we have a portal for information sharing. Again, that's part of that redistributor facilitator role that the ACSC plays. It is really a clearinghouse for the information that we're sharing on a biweekly basis.

So the benefits—again, we talk a little bit about that during the day. The face-to-face in-person meetings establish trust, and it takes time. So we've had people who have been in the ACSC since the beginning, and we have new participants who have been coming in over time. And you do see that sort of emerging trust from the new participants as they join. Those of us who have been there for a while understand how it works, understand the model, understand that the information we're talking about is to be shared amongst the participants. We don't attribute any conversations outside of the ACSC. So there definitely is a large willingness to

share, to collaborate, and again, we filter the information that we're talking about to those things that we think are really actionable and really useful to each other. We usually don't go in there and talk about things that really aren't going to affect our ability to better protect ourselves.

Now, with that said, there are legal agreements. I mean, if you work at the Federal Reserve Bank of Boston, pretty much everything we do has to be bound by a legal agreement, and so there are NDAs in place to formalize the protection and the participation there. But really, the benefit is from the face-to-face conversations.

Cross-sector participation does highlight the different views, perspectives, approaches, and priorities. I guess when we think about cross-sector, we can sort of wave our hands and say, "It's a good thing. It makes sense," but why does it make sense? I think what we see within the ACSC is that there's a diversity of opinion, of approaches, of environment. When you talk about having a government organization come in with one view where you have an organization like MITRE who has a different view, the Federal Reserve definitely has a different view, right? So we all are looking at protecting different things. Our priorities are different. I know from the Fed's standpoint, you know, we have an enormous amount of transactions that go through the Federal Reserve on a daily basis that we need to protect. So those things, we think about integrity. We think about keeping service available. We think about protecting information. When you have other organizations that may have different priorities, universities have different priorities. So our ability to get together and talk about what we're focused on, what we're doing, and getting those different perspectives really helps us all, right? So we're not all the same school of thought. We're not all coming from the same place and saying, "You know what, we've all heard the same thing from the same people year after year, and we're all doing the same thing." Here we are definitely getting a diversity of opinion.

And then we get the benefits of small groups. Again, once you get an enormous group together who is trying to share information, you start getting sort of that—I don't know—an unfiltered set of information that may or may not be useful to you. When we get small groups, we can really question each other. We can test each other. We can poke at each other, and our ability to really sort of filter things down to information that's useful is really, I think, much more achievable when you have smaller groups.

What that right size group is, I think we're still working through. The ACSC started very small. I don't know the number of participants, but it definitely has grown over the years, and so you really have to think about how many people you want in a room before it becomes too large. And again, we have that ability to ask questions and have conversations.

Now, so those are the benefits. The challenges sometimes we get from a group like ACSC is that not everybody comes in—and again, this is with any group. Not everybody comes in with the same level of experience, with expertise, with an ability to contribute. So you may have people who are clearly experts in the field who know how to manage incidents, know what to look for, and they tend to be the leaders within the ACSC, and they are really—you know, they

are mentoring I think some of the other participants. Other participants come in, and they are much more in a learning mode. They are there to learn from each other, ask questions, but they may not have the ability to really, I guess, drive the conversations as much as others. So when we think about what the ACSC does or any sharing group, we really have to think about who the constituents are and what the expectations are when they come into that organization because it's very difficult to bring people together and invite participation and then manage the fact that not everybody is going to be at the same level and is going to be at the same level to actually get things done or participate or educate each other. So those are things we constantly work towards when we even think about the small group approach for ACSC.

In terms of feedback, this is surveys that were done a while ago. The vast majority, I would say from ACSC membership is that they are getting actionable intelligence. So again, they are not just learning about neat stories and things that are going on and saying, "Hey, that was interesting. I heard a great story. I'm going to break it back and tell people." It's actionable intelligence. It's things that they can go back and do, and part of that is what we're learning about in incidents, what we're learning about in terms of sharing what our programs are, what we're doing in terms of technologies where we're deploying, anything that we can talk about to say "Hey, this works" or "This doesn't work." People are bringing that back and using that within their organizations.

You know, people are saying that this is helping them with their security posture, helping them to defend themselves, and they feel that their organizations are more secure. And as you'll see, 63 percent believe that their skills are getting increased by participation. Again ,that goes back to who the participants are and what each one of them are getting out of it. So certain people are coming in there, and they are definitely helping to drive the conversation and educate others. Other people are really getting the benefit of having their skills increased.

In terms of recognizing the value of the ACSC model—and I am definitely not going to read through all of these things, but, you know, we are getting more recognition in terms of that small team model where we are looking at getting more conversations with our participants, feeling that we are really getting actionable intelligence out of this, out of the organization. And again, this is small scale. I know that there are organizations who are looking at replicating this kind of model within other geographic locations because, again, part of what we're looking at is those face-to-face meetings between people. And once you start having large geographies involved, it makes it more difficult. Even if you're starting to do it over video and across the country, it's still more difficult when you do that than when you have people in the same room. We take breaks. People congregate. People can talk about different things, even informally. That's a hard model to do when you're not doing it physically.

And I think—I know we have a short time, so I think that's pretty much it. Charlie Benway, who could not be here today, he is the Executive Director of the Advanced Cyber Security Center. So I'm leaving his contact information here. It should be made available. So if you have an interest in learning more about the Advanced Cyber Security Center, definitely contact Charlie. He's local, here, but obviously he's available at any time.

I wanted to talk about the ACSC and participation in the ACSC, but also to talk about the model, so how is the ACSC organized, how does it work, and is that something that other people could walk away with and think about when they're thinking about ISAOs, what they can do in those kinds of areas. Again, if you'd like to talk to me, again, we're a participant. We definitely chair the ACSC organization. If you'd like to contact me and talk further about our participation and how the Federal Reserve gets benefits out of that, definitely contact me. I'd be more than welcome to invite any conversations.

If anybody has any questions, I know that we're short on time, but if anybody has any questions about ACSC or small groups? Yes.

ATTENDEE: With all respect, how much money does it cost to run the organization, and where does your money come from? If you can't say—

MICK COSTA: So there is a fee to participate in the Advanced Cyber Security Center, and I'll let Charlie talk about what the actual costs are. So the ACSC, I believe, is funded partially out of Mass Insight, which is a local organization, but it's primarily through the membership of the participants.

ATTENDEE: What's the cost?

MICK COSTA: I actually don't have that cost information on me. I'm going to leave that to Charlie because I'm not sure. I think it depends on different levels of participation, but I am not sure of the costs.

ATTENDEE: Again, I'm not trying to pry but—

MICK COSTA: Sure.

ATTENDEE: —ball park? Is it like a million dollars a year?

MICK COSTA: It is much, much, much less than a million dollars a year.

ATTENDEE: Is it 500,000?

[Laughter.]

MICK COSTA: It's much, much less than $500,000 a year. No, really, because when you think about it, we have—you know, even though I know you think about the Federal Reserve and maybe we're printing money to go join this—

[Laughter.]

MICK COSTA: Which we don't print money. But you think about we have universities. We have Boston University. We have MIT. We have Northeast, and we have UMass. So, I mean, we have organizations there that do not have the size wallets to be able to spend big money on this. So this is something that has participation from—I would say from organizations that don't have giant pockets.

I will say that a couple months ago, I gave a talk at actually the North Shore Chamber of Commerce, so one of the chamber of commerces that's local, and that's much smaller organizations, right? And one of their questions was "How do we get the benefits of an ISAO? Right? So we're small. We're mom-and-pop. We're not a university, or we're not certainly the Federal Reserve. We're not a giant organization," and that's a difficult question to answer. So we're definitely not at the level where we can have a three-person company come in and join us, for they probably couldn't afford it, but also it doesn't take a JPMorgan, Chase, or a Federal Reserve to join either.

ATTENDEE: So the answer to that gentleman's question, it is posted online. So I feel like I can say it to folks here.

MICK COSTA: Sure.

ATTENDEE: [Speaking off mic.]

ATTENDEE: [Speaking off mic.]

MICK COSTA: So I would say if we think about the Advanced Cyber Security Center—and they sort of have those three pillars of what the ACSC does—one of those pillars is a cyber threat sharing. Other ones, another area is R&D. It's education. The other one is legislation. So there's—the funding for ACSC isn't just to do the cyber threat sharing. So it is to cover the entire bulk of what the ACSC does. If you were standing from an organization that was purely going to do the cyber threat sharing, the cost model would probably be different.

MIKE ECHOLS: Thank you.

MICK COSTA: Thank you.

MIKE ECHOLS: Thank you, Mick. All right. Thank you very much.

[Applause.]

[Break.]

Workshop Breakouts
Track 1: Forming ISAOs Panel

ROMAN DANYLIW: [In progress]—your seats. So I'd like to welcome everyone to Track 1, which is the Forming ISAOs track. Just in case you're in Track 2 or 3, that's either in the Learning Center or Room 120.

This is the start of us diverging from talking things in the generally to really rolling up our sleeves and getting into the, getting into the specifics, so with this desire to really get your feedback on the Executive Order, the execution of it, or recommendation you may have. DHS organized all the different topics into one of three tracks. We are focused on things like models for creating ISAOs, how they might be used, and figuring out what some of those lessons learned might be.

Logistically, what we're going to do is first start with a panel of organizations and individuals that have a lot of experience with information sharing, and they may be your future partners at some point. We're then going to break for lunch and have two breakout sessions. The first breakout session is going to focus on topics related to what relationships ISAOs could have with their constituency, with the government, and what are the ways in which these ISAOs may ultimately be designated, and how should some of the various baseline standards be defined. And then the last breakout session we're going to be largely focused on lessons learned, the incentives, and what might be shared visions and other challenges and opportunities to forming ISAOs.

The very key thing to remember here is that DHS wants to hear from you, wants to hear about your opinions on this, and you speaking up is an opportunity to provide that feedback. Everything that is said here is going to be, if it's in this auditorium is going to be recorded. In the other rooms it will not be. But all of your comments will be aggregated into a white paper, and that white paper will distill the various themes and ideas that were shared here, and the intent ultimately would be to share that a couple of weeks after this event, first, of course, with DHS, with you as the participants, with the general public, and it will be the basis of concrete feedback given to the standards organization.

One logistical piece of help. Good feedback and a good, high-quality white paper is going to come from your comments, but one logistical place that would really help is that my colleague Jeff Apolis, sitting here up front—if you could raise your hand—is going to be helping us with the note-taking, so just in case we might have to find you later, if you could perhaps speak your name or your affiliation. That will help us locate you if there's something follow-up that we, we might want to have.

And with that I want to turn it over to starting our panel. So chairing our panel is my good colleague, Carlos Kizzee, who is the Executive Director of the Defense Security Information Exchange. Carlos, please come on up and help us get this panel started.

CARLOS KIZZEE: Thank you. Thank you, sir. First and foremost, let me give a reminder to our esteemed experts on the panel. I'm not so sure. I was standing in the back, back there, and especially with the road noise from outside you might want to speak into the microphone

because it's probably a little bit hard to hear in the back. Likewise, if you can't hear, just give us a signal or something like that, so, so we will know.

So Roman introduced me, Carlos Kizzee. I am the Executive Director of an ISAO, the defense industrial base's Information Sharing and Analysis Organization for Cyber Security, the SIE. One thing I want to kind of stomp the foot on, as we're talking about ISAOs—there is nothing new about ISAOs, right? The term has been around since 1998, 1999. I mean, the Homeland Security Act actually has the definition in it, and that was written in 2002, or published in 2002. It was actually written probably around 2000. So information sharing analysis organizations have been defined and have been in existence, and many organizations—Mike Arceneaux right there represents one—many organizations, ISAO organizations, have been around since 1999, 1998, and so on. Mike is the, the Director of the WaterISAC. So ISACs or ISAOs.

And there are today—I'm not sure, Roman, if you would be able to tell me. I know we, the Defense Security Information Exchange, signed an agreement with DHS, and we named our legal and organizational name as the DIB-ISAO, but there are other organizations that today are calling themselves ISAOs and are, are standing up and being established. So I want to be really, really clear that this concept that we're talking about, not a new concept, and it's important for us to realize that what we are talking about is not a name or a title. It's a functional set of activities that have been going on for a long time.

And how do we improve that? Our panel represents two government agencies, an FFRDC and a nonprofit organization, all active in the area of cyber threat intelligence and in partnerships and partnering. I'm the moderator of the panel, and in that role I, I also represent an ISAO, as I've said. We're not here as a panel to discuss or to inform on how to form an ISAO. Odd, because isn't that the topic of this, this discussion? What we really want to talk about is informing aspects of ISAO formation. We want to talk about what are some of the things that you might need to do, and there's one particular area that I really, really want to tease out with this particular panel.

When forming an ISAO, a key consideration that you have to decide, and have to come to grips with, is, whom is relevant as your partner? Who should I connect with and why, for what purposes? And I think that that "whom" is one of several very, very important things, because the "who" I'm going to connect with might define what particular models, like the last speaker was talking about, what models for ISAO formation. Am I going to be a distributor to other partners? Am I going to be a facilitator? That type of thing. And so that's why having a couple of government agencies or entities who partner with ISAOs, with ISACs, and with industry parties is a good idea.

Also, whom you partner with may also define particular opportunities and particular challenges for you, as an ISAO, things that you want to take into account and to consider as you're forming that organization, as you're developing and maturing your business processes and operations. And, you know, I don't want to underestimate what, what Larry asked, you know, the question he asked—how much does it cost? I mean, what is that I'm going to do? I mean, there's a

whole lot of factors that you have to consider. What I want to focus on here is, who are some of the partners? Who are some of the entities that you're going to connect with, and how should that happen, and what are some of the concerns with making that happen?

So, we have a panel of folks, and I will introduce them, starting from your left, my right. Brian Scully, the Deputy Director for Policy, DHS Infrastructure Protection; Bruce Bakis, Principal Engineer for MITRE; Stacy Stevens, Unit Chief, Cyber Division, Federal Bureau of Investigation; and Maria Vello, the President and CEO of the National Cyber Forensics and Training Alliance, which really isn't fair because they're kind of double-dipping here, but they're worth it. What a great organization. They've been a really effective partner for many of us, for years.

MARIA VELLO: I tried to get on three panels.

CARLOS KIZZEE: Yeah. See, and, and if you could be in two places at once you could be in one of these two breakouts.

So what we're, what we're going to do—and here's how this is going to flow, no surprises—I want to give you an opportunity to get to know them. So I'm going to ask two or three questions of them as a panel and let them answer individually, and poor, poor Brian, we'll start with Brian and work our way down. After I ask those questions, I have a series of questions here that are really boring and softballish and easy for them to answer. If you don't have questions, I'll ask my easy, boring questions, but I'd really encourage you to ask some hard, tough questions, because these are really, really smart people, well-seasoned people.

So that, that's the process we'll go, and I would like very, very much to—when you ask a question, I don't know if we're going to hand the microphone out—when you ask a question please be considerate that the room is big and the acoustics are horrible. So speak up on your question, and, panel members, if we don't have a good feel that everybody has heard the question, if you don't think, maybe we could repeat the question when we give the answer.

The last thing I would ask if you do ask a question, please give us, if you're willing to do this, the opportunity of understanding who you are. Just kind of introduce yourself so the panel knows, you know, what you're speaking from. And given what Mike has said before about anonymity, if you'd rather not do that you're welcome not to do that. But I really would like to give the panel the opportunity of knowing whom they're addressing, so that they can answer the question appropriately.

Does that all make sense and that's all fair?

So let me now ask the panel, who are you and what do you do? And, sir, I'll start with you.

BRIAN SCULLY: Great. Is this on? Am I good. Oh, sorry. Pulled it right off. I'm not going to touch. So good morning. My name is Brian Scully. I want to thank Mike for inviting me and Carlos for facilitating the session. It's a great opportunity for me to, to get out of Washington

for a little while, which is, which is always good. So as Carlos said, I am the Deputy Director for Policy and Strategy at the Office of Infrastructure Protection, which is within DHS. We are actually within the same organization within DHS as the cyber folks, so Mike's team. We're just a different entity within there. So they're focused on cyber. We're a little heavier focused on the physical security side of infrastructure protection.

The reason I'm here today, and, and the core of the work that I'm doing, a big piece of the work I'm doing now at, at Infrastructure Protection, is developing a threat information sharing framework, which is looking across—and we're doing that in, in partnership with the FBI. I don't want to throw out all sorts of—so the, the Federal Government has a proliferation of strategies. One of those strategies is the National Strategy for Information Sharing and Safeguarding, which many of you are probably aware of. Within that there's a, a call to develop this threat information sharing framework. It talks about how the Federal Government shares threat information with critical infrastructure owners and operators.

So DHS, along with the FBI, are co-chairing, a, a—it's both an interagency and it includes private sector, it includes sector partners, and it includes nonprofits, state and locals, to develop this framework. Essentially what the framework is going to be is more of a guidebook. So we're trying to identify a niche space. There's a lot of—everybody's doing information sharing these days, so what was something that we could do to, to provide some value. So it's, it's more of a guidebook in a sense. We're going to try to identify the existing systems and mechanisms that are used for the Federal Government to share information with private sector owner/operators—well, all owners and operators. We often say private sector but it's sustainable for governments also, and quite a bit of infrastructure as well as the Federal Government, for that matter.

So how is, how does the Federal Government share information—threat information, in particular—in cyber and physical threats, not natural hazards and things like that, with critical infrastructure owner/operators? We've had a few meetings. We've invited Mike to, to one of our meetings, and so we're trying to lay out what the current systems looks like. How do we currently share information? How does it currently work? And the idea is that people can really take a look at this and understand how the Federal Government is pushing the information out and how we're getting it returned, so if they want to plug into the systems that exist, that there's a clear and easy way to understand how to plug into those systems. We can talk more about how ISAOs fit into that, which is obviously a clear connection. The ISAOs would be a core part of the framework, as well as the ISACs.

And so that's roughly what I do. I don't want to overshoot my time, because we also have lunch following this, so I don't want to get in the way of that either. Just by way of background on myself, though, I've been at DHS since the beginning. I've spent 8-1/2 years at FEMA. I've also spent 3 years at the DHS Office of Intelligence and Analysis, and I came out of the private sector to join DHS, so just some history.

CARLOS KIZZEE: Bruce, same question. Who are you what do you do?

BRUCE BAKIS: Well, first of all, thank you to the Department of Homeland Security and Carlos for helping to prepare this panel. I am Bruce Bakis from the MITRE Corporation, and I'm a cyber engineer, and I'm focused on—many of our corporate initiatives are relating to cyber, in particular, to helping to form partnerships. Consistent with MITRE's mission of operating in the public interest, we are helping to catalyze the number of partnerships, similar to the Advanced Cyber Security Center. We're doing that across the country and even internationally. So that's really part of our focus.

In terms of the importance of partnerships to MITRE as a corporation, it's really one of the key pillars in MITRE's fundamental cyber strategy, which includes threat-based defense, operational innovation, resiliency, and partnerships is really at the cornerstone. And so we believe, much as we've heard today, that there's much to be gained by operating in terms of a team sport type of approach, and MITRE is a member of several defense-related consortia, as well as a number of others. So we probably participate in five or six sharing consortia, and we derive tremendous value from those relationships.

CARLOS KIZZEE: Awesome. Stacy, who are you and what do you do?

STACY L. STEVENS: Well, first of all I'd like to echo my panelists' remarks by saying thank you to you and Mike for inviting me to be on the panel. I am a unit chief in Mr. Riggi's Cyber Operations section. It was formed back in 2013, in order to decide how we want to share information with the private sector. Obviously, this has been going on with our field offices, at the tactical level, but what we really wanted to do was enhance the way we work with the SISO, C-suite level individuals from larger corporations in the five, top five what we determined were critical infrastructure, and that would be banking and finance, energy, transportation, IT, and coms. And we also added public health a few years back.

So what we really try and do is reach out to the folks and bring them and give them classified threat briefings, and give them an understanding of what we do and why we do it, and some of the limitations that we have for sharing information. Some of that can be, if it's an ongoing investigation or an ongoing intelligence matter. But we really wanted to open up the coffers and say, "Hey, here's what we know about a specific threat. Can you help us and let us know what you know about that threat?" As Mr. Riggi did say, it's a puzzle, and I know, in the past, we had always gotten the comments that "When we work with federal law enforcement or other law enforcement partners, it's like a black hole. We give you information; we don't get anything back." A lot of that is because we may need what you have out there, in order for us to figure out what really is going on. So that was part of the reason and the strategy behind developing my unit, is to really get out there and say, "Hey, we need your help. You need our help. How can we do this together?"

We also have another unit within the operational division that does outreach, and that's our Cyber Investigative and Resource Fusion Unit. That sits in the Pittsburgh field office and it sits with the NCFTA, and, again, I know, Mister, or Carlos had said about beneficial it is having the

NCFTA, and it's crucial for us to be a part of it because we're able to look at national-level initiatives with our private sector partners, with other law enforcement, with academia, and say, "How do we want to prioritize and how do we want to address these threats?" So we do that as far as outreach is concerned too.

We also have the InfraGard Program. We program manage that. We provide resources out to the field offices in order to support the InfraGard Program. Again, that is individually based and as long as you have some sort of affiliation with the private sector, as far as the critical infrastructure sectors or academia, you can become a member.

My opinion is that that's probably consider an ISAO as well. I'm not sure if, at the national level, we do have a national level program, and then we also have the 83 chapters. So I don't know if they would be one big ISAO or separate ISAOs. But it is going to be interesting to see how we should form and why we should form these. Is it just to information share? Is it going to be the ability to really work on some sort of imminent threat or look at some sort of national-level cyber matter that needs to be addressed? So it will be interesting to see how these all develop as they form, so I'm looking forward to having a conversation about this.

MARIA VELLO: Good morning. I guess still good morning. All right. We're still there. I'm Maria Vello. I'm the President and CEO of the National Cyber Forensics and Training Alliance, so NCFTA. The name certainly is not indicative of what the NCFTA does, and I'll talk a little bit more about that. But Carlos, I would be remiss if I didn't say thank you for inviting me. My fellow panelists, thanks for being here on the panel, and I'm glad to be here. I'm honored to be working with you. And thanks to the audience for really listening and really taking, you know, an interest in the ISAO and what's going happen and how this is going to be formed.

But the NCFTA is located in Pittsburgh, Pennsylvania. We are a nonprofit. We're a 501(c)(3). You know, our mission is really to work with government agencies, academia, private industry to combat cyber crime on a global basis, or neutralize cyber crime on a global basis. So what we do, we've been in existence for 13-plus years. I really think that that, in my opinion—and this is my humble opinion—that we are one of the poster childs for, you know, information sharing, and it's not just information sharing. It's really resource sharing too, because if we can, say, share information, and we can share resources, then we can save everybody time and cycles also. And I also challenge you to say, when we talk about information sharing, what do we mean, you know? Everyone talks about information sharing, but is it just indicators of compromise? Is it preventative, proactive? You know, because I think it's too late if we're looking at this and taking the approach of after-the-fact.

So one of the things at the NCFTA, that we do, is really we look at, you know, identifying the threat, looking at who's doing what to whom, how are they doing it, where are they doing it from. As Matt mentioned this morning, we get information from private industry. We take that information. We anonymize it. We sanitize it. Our analysts, who a lot of them are multi-lingual, they, you know, look, go search across the Internet through open source social media tools to add intelligence to that information. We turn the information into intelligence that's

actionable. And you hear the word "actionable," so things that we can give private industry, that they can be preventative and proactive—how do you put up your defenses to prevent something from happening? How do you make sure that you have a flag in your systems, to alert you when something is potentially going to happen?

And then we also, you know, work law enforcement to, you know, give them actionable intelligence. They have their—you know, we save them time and resources. We kind of find the needles in the haystack, to identify where we think the threat is coming from. They replicate. They duplicate. They have to enhance everything. But they're the folks that they have to go out, seize assets, seize funds, and make arrests. If they don't do that, then everything we're doing from an information sharing perspective is for naught. We've got to be able to neutralize the crime. You know, we've got to be able to stop it from spreading, and the only way to do that is by, you know, putting handcuffs on these people. And you have to have strong prosecution. So I think there's a number of different areas, though. If we want to be successful as ISAOs, as we start to look at how these form, or what it becomes, what it takes to become one, we have to think about that, that secret success or that recipe for success.

We are cross-sector, industry-based, so we look at, you know, we can see one case of fraud and we can see it touch, you know, six, seven, eight different industries, and because we're working across industries we can put that piece of that puzzle together. As Mr. Riggi and, you know, Stacy just mentioned, it is a puzzle, you know, and it's taking seemingly unrelated data, or insignificant data, and putting together all the pieces to put the last piece of the puzzle, to identify, you know, the threat landscape and come up with a solution.

So today, I mean, our model is being replicated around the globe. We have JC3 in Japan. That's the most actively and has said on their website, you know, they're using the model of the NCFTA to build their entity, and have built their entity. Singapore, yeah, the Interpol is replicating the model of the NCFTA. You have Canada, you have UK, you have Germany—a number of organizations that are replicating the model of the NCFTA. It's a global problem that we have, and NCFTA works with not only domestic and, and, as well, private industry and law enforcement agencies, but global private industry and, you know, law enforcement agencies. It's a global problem. None of us are immune. All the threats don't emanate from the United States, and certainly all the threat actors, you know, do not come from the United States. So I think we have to be aware of this on a global basis also.

You know, every time—everything we do as we try to be preventative and proactive, we're actually trying to protect people's brands, reputation, and the economic impact. This is a—yeah, the problem that we're addressing is not just, you know, a problem in the U.S. It's global, and right now it's challenging everybody's economic infrastructures. So we need to, you know, look at this very, very closely. Perhaps we need to take a step back and examine what's working today, and I think that's what, you know, the DHS is trying to do, but let's leverage every model that's out there. Let's take, you know, the best practices, the lessons learned. As we work with industry and private industry, we are, you know, building lessons learned. We're bringing in regulators to talk about and bring clarity to some of the rules and regulations

around sharing. We're helping people share tools. If you've been hit by some sort of emerging threat or DDOS, if I've built a tool let me share that tool with you, so you can protect, you know, not only the enterprise companies that have the time, the resources, the experience, but let's share that tool down with some of the smaller companies so that they can put up their defenses, because they need help. They don't have the same expertise that some of us do.

And then I also think, you know, we talk a lot about trust and trusted relationships. You know, I'm a firm believer that you don't build trust; you earn trust. And the NCFTA, the model of the NCFTA was built on trust and trusted relationships. Matt mentioned this this morning. You know, we've earned people's trust. We say what we mean, we mean what we say, we say we're going to do something and we do it. If we meet somebody at a conference, we're not going to just bring them into the fold, because that's not somebody that we know. You know, the people that we're working with are trusted entities. They're people that know each other, have known each other for a long time.

Security community is a very tight-knit, small community. You know, we're working with subject matter experts around the globe, so sharing, you know, information, best practices, and tools. You know, that's what we have to continue to do. And, you know, at the NCFTA we tell people when they come to visit the NCFTA, you know, when you come, the enemy is on the outside. It's not on the inside. We have zero tolerance for competitive behavior. The worst thing that can happen to us as we start to form these ISAOs is that we compete, and we pull people away from each other. It cannot be a fragmented approach. The criminals that are out there, they're organized, they share seamlessly, they know more about us than we know about ourselves. So we have to be careful in that aspect.

And I also think that, you know, the NCFTA, it is—we have a common goal. When you come we say bring—you know, bring your information, bring your intelligence, bring your emergent threats, share that with everybody. We have a common goal. The enemy is on the outside, so all oars in the water, rowing towards that common goal. So, you know, we have multiple, you know, entities in cross sector that are some of the top brokerage firms, financial firms, you know, pharmaceutical firms, that they're not marketing. It's about protecting, and that's what we do at the NCFTA. We protect. We share information, you know, critical information, because it can be—you know, what do we share? There can be anything ranging from a cyber financial crime to counterfeit goods that are getting into our supply chains. You know, so we have to look at this across many different aspects, plus the botnets and what's happening from the botnets, that are very, very sophisticated and can move laterally, and they're very dynamic.

So we tell people, leave your ego at the door. Let's all work together for the common good and let's share and focus on what you can share, not what you can't, and come with the attitude of giving more than you're going to take, because that's how we'll all be successful. The two-way sharing, as Matt mentioned this morning, is critical. I tell people there isn't any relationship out there that if it's only one way, that it works. I don't care if it's your wife, your partner, your friend. One-way sharing and one-way relationships just don't work. So I think that's key, also, to the success of the ISAOs. Thank you.

CARLOS KIZZEE: And now let me point—and we're going to come back to Brian—I want to now ask the question in a slightly different way. Earlier someone raised—used the term "value proposition." And so what I'd like each of the panelists to address, if I am an ISAO, a newly forming ISAO, and I want to connect with your organization, can you briefly articulate for me what is your value proposition for connecting with me, an ISAO, and what might my value proposition be for connecting with you?

BRIAN SCULLY: Sure. At the Office of Infrastructure Protection, our mission is to enhance the security and resilience of the nation's critical infrastructure. So from our perspective, the value proposition we offer—and I think this probably goes for a lot of federal agencies, departments and agencies—is we have access to a lot of information and data that the private sector does not have access to. We have access to intelligence reports. We have access to a large number of subject matter experts. So we have access to information and data set that the private sector may not. So that's one part of the value proposition.

We can form trusted relationships across different sectors, different entities, so at the Office of Infrastructure Protection we work closely with all 16 critical infrastructure sectors. There are governing mechanisms that allow us to move information and data through those sectors. And so the relationship side of it, we have established governing models, established governing systems, is another piece, I think, to the value proposition that we offer. We can also offer training, technical expertise, and things like that. I could go into the whole IP sales pitch but I won't. I won't bore you too much with that.

From the flip side, though, we also recognize that the private sector has a significant amount of expertise, a significant amount of information, and a significant amount of data that would be valuable to use, as the Federal Government, to help us make decisions on resourcing, on policy, on all sorts of things. So, as was just stated, it's a two-way sharing of information, a two-way relationship that needs to be built. That is critical, and I think we both have something to offer each other. So I think the Federal Government has a lot to offer in terms of data, technical expertise, information, relationship management, governance mechanisms. You look at PCII. We have some ability to protect data and information that is shared through different mechanisms. We have different counsels and legal mechanisms to allow you to share information and bring private sector and public entities together to talk. So there's a lot of value there, and, of course, as I mentioned, you know, from the flip side, we don't, we don't know a lot of things. There's a lot of expertise and knowledge in the private sector that is of great value to the Federal Government, and we need to be able to tap into that.

CARLOS KIZZEE: Awesome. Bruce, you mentioned that MITRE is a member of multiple consortia and other organizations. Could you talk also—you know, what's the value proposition for me connecting with MITRE as an ISAO, and for MITRE connecting with me?

BRUCE BAKIS: So MITRE has quite a bit of lessons learned from their—its experience in terms of participating in information sharing organizations, and even more as we help catalyze some

of these, really, across the country. So we've offered, on our public website, a series of observations that are called "Lessons Learned and Challenges." It's in a series that we have under, under the cyber security space, where we're talking about partners with purpose. And so we've captured some of the lessons learned and challenges there.

One of the things, you know, Carlos, you said, in terms of, you know, what is the fundamental role and the essence that, you know, an organization or an ISAO would offer, as simple a question as that is, people have difficulty in articulating that. Maria did a really great job of articulating essentially the value proposition of the NCFTA. As we work with, in other regions across the United States, in particular the larger the region the more difficult it becomes, is to be able to articulate what is your mission or your value proposition.

So what we're seeing in these large regional, even statewide ISAOs is a little bit of paralysis because they want to be everything to everyone. So they have very, very broad mission visions, which actually go beyond, just, you know, sharing information and analyzing information. And we talk about economic development. We talk about research and—cyber research and development. We talk about sort of influencing policy at a national level, or even a local level. Those are all excellent missions, but the broader the mission, the more difficult it is to get, really, traction on I think why we're here today, to really focus on the information sharing piece.

So as we talk to organizations, we say you need to essentially be able to articulate what your mission is and your value proposition on a 3-by-5 card in a couple of bullets, and to the extent that you can't do that, it's great to think big, but we're saying to people, "Think big, start small, and move quickly."

CARLOS KIZZEE: Very good. Stacy, likewise, I mean, the Bureau has a lot of initiatives and programs that, you know, working with DHS and independently as well, in regard. What's the value proposition for me, as an ISAO, to join, but also what's the value proposition to you for me connecting with you?

STACY L. STEVENS: Right. So we are in a unique position where we have investigative and intelligence-collecting authorities in order for us to be able to address counter-terrorism matter, counterintelligence matters, and cyber matters. So because cyber is more of a vector, for criminal activity, for terrorist activity, and counterintelligence activity, we're in a unique position to kind of put all that information together and provide that information out to the private sector. Why are you being targeted? How are you being targeted? Are you being targeted by criminal actors? Are you being targeted by a nation state? Are they changing their tactics, techniques, and procedures? These are the things that we can provide you when you work with us.

Obviously, we'll need to know what's going on within your company. Why do you think you're being targeted? I can give you an example that we recently talked to a company that had recently experienced an intrusion, and they said to us, just an off-the-cuff remark, "Hey, would

it be interesting for you guys to note that ourselves and a couple of other companies were getting ready to do some business at a particular nation state?" Bells went off, right? Yes, yes, that would be very good to know, because then we're able to say, hey, were you targeted because of this? Are you partners going to be targeted in the future? So then we're able to warn the other partners, or the industry as a whole. So I think that that is a good proposition for the private sector to work with us, is the fact that we can look cross-threat and be able to say, "This is why you're being targeted."

In order for us to be able to do that and to collect information, again, cyber is unique. Counter-terrorism or terrorist activity, if you're a farmer and you sell, you know, something that, that a terrorist may use—fertilizer or something—you come to us and you say, "Hey, somebody just bought a bunch of fertilizer." Thank you very much. We call that a trip wire. It's a tip. We don't really have to come back to you and say, "Okay, this is why this person bought that, and this is what we stopped."

But in the cyber arena, we need to know what you have and why you think you're being targeted, because you know much more about your networks than we do. So in order for us to build our intelligence capability and our investigative operations, we need your help. So I think that two-way information sharing partnership, trusted relationship, is essential in addressing cyber threats.

CARLOS KIZZEE: And, Maria, I'd ask this question of you, of NCFTA, probably in a little bit different way. Let's say that I'm the ICS ISAC or the automotive ISAC, or the water ISAC, or the defense industrial base ISAO. What's the value proposition for me as an ISAO partnering with NCFTA, and what's the value proposition to you for me partnering with you?

MARIA VELLO: I'm going to say it depends. I'm going to ask you, you know, what your mission is. I'm going to ask you what your objectives are. I'm going to try to find out more about you and what you do and how you do it. I think that there's probably going to be multiple ways that, you know, we have—maybe you have skill sets that we don't have and we have skill sets that you don't have. How do we share those skill sets and share that resource so that we don't duplicate efforts with what we're doing, so we save time, cycle, money? Because we work cross-sector with all the different industries, you know, everyone knows, everyone has networks, everyone has people, everyone has issues. They don't stay in one industry. They leverage the same tools across multiple industries.

So we're going to talk to you about what we're seeing. What are we seeing from an emerging threats, whether it's with our peers in the agencies, with FBI, Secret Service, Customs and Border Protection, HSI? What are they seeing? What are we seeing? What's our industry partner seeing—because industry, quite frankly, has the best information. No matter what, they have the best information. You know what's on your network, you see who's attacking your network. We're going to be able to tell you emerging threats, and then hopefully you're going to give us some of the same information back.

We can't be all things to all people, but, you know, we certainly want to be laser-focused on, you know, how we can help you. So we're going to find out a lot more about you, look for ways that we don't have to duplicate efforts, and save everybody time, cycles, and money, because nobody has enough resources to go around.

CARLOS KIZZEE: Awesome. Very good. So here's now where I start to ask some questions that are probably too easy and are not as good as the questions you're going to ask. So if you have a question, I would invite you to just stand up and raise your hand or somehow signal us. I don't know where our mics are. But while you're preparing a question that you might have—I see one right there. Sir.

JONATHAN GOLDER: It's not so much a question, but it's a comment followed by a request, and I'd maybe question how you guys might answer that. One of the big issues that I run into so just to put—I'm John Golder. I'm with Discover Financial Services.

CARLOS KIZZEE: Thank you, John.

JONATHAN GOLDER: I run our Enterprise Intelligence office that I'm standing up. So I'm used to working in the intelligence community. I'm used to working with intelligence media. One of the things that I really see is going to be an issue is taking this past the security crowd, taking this past the people that are used to dealing with this, and getting it to the see levels, getting to the other guys who are not trained intelligence consumers, they're not used to having these sorts of fees, and they're not used to this sort of information. We're used to—you know, those of us that come out of a government or military background are used to dealing with people that are used to this sort of information.

What I'm asking is, who's looking at methods to train intelligence consumers, intelligence producers, and intelligence users in these company, because—for example, in my company, I'm trying to move that direction internally, but not all companies are going to have that in-house expertise to do that. So what are we looking at? At steps to try and train people to be effective users and then effective participants and then eventually grow out their own capacity, because it's got to be a qualified run, and what are the mechanisms we're looking at for that?

CARLOS KIZZEE: So, for the panel, anybody want to jump on that question?

MARIA VELLO: I'll take it. So to answer your question and be quite honest, I don't think we're doing enough. I think we do some of it. You know, we've brought in, you know, when we've had different—we've done Security 101, you know, for people that really just didn't even understand, you know, how to spell "firewall," let alone, you know, what an IDS, IPS and what they should be doing on their network. But that's only one component. The network is one component of everything that happens.

I mean, you look at, you know, the—so it's fraud. It's, you know, emerging threats. It's new schemes, you know, how are they leveraging, you know, what are they doing with counterfeit

goods, how are they hurting your brand or your reputation? So we do some of that. I don't think we do enough. I think that, you know, we don't have enough people. There's not enough people out there right now, in the security field, that really understand, you know, the challenges or understand the, the, the issues that we're having. But they're not going to school. They're not being trained.

So I think everyone has a challenge with resources. I think if you look at what the White House is doing, that's one of their key challenges. You know, we do human capital development, but we do it more on the intelligence analyst perspective, not on the network security. So I think there's multiple lanes that we have to look at. I think we have to do a lot of it. I think that's, you know, where DHS could play a huge role, you know, in getting more people trained and more people educated.

STACY L. STEVENS: And I would like to kind of echo what Maria is saying and give you an idea of the challenges with state and local law enforcement too. So not only is it private sector, it's state and locals, right? So a lot of them have no experience whatsoever and ignore the cyber threat, because politically, I can be a mayor or I can be a police chief and say, "Hey, I've stopped so many robberies, I've stopped this." How do you say you've thwarted, you know, a scam that started in one city and is hitting your city? So we've provided, within the FBI, something we call Cyber Shield Alliance, where we've set up a portal in order for state and local law enforcement be able to get some of the training that they need. So they can go on and sign up for certain things and get training.

Again, we're not doing it with the private sector as well as we should. A lot of what we do is bring the private sector in and say, "Okay, these are the threats. This is what you should be looking at." And we have had SISO say, "Thank you. Thank you for showing the CEO that cyber is a real threat, and that we do need to protect against it, and that it's going to take a lot of money to do so."

But I do agree with Maria. There could be more, and I'm not sure who should be in charge. I do believe, yeah, DHS would probably be the best place to, to start that, as far as the protection side of the house, but I know it is a challenge for us, and, again, like I said, we've got to look at our state and local law enforcement partners, which is a challenge as well.

ATTENDEE: There's kind of two layers to that piece. One is, yes, at the, you know, building security to be understood as being critical, and there's a monetization factor that the government often doesn't think about in that sense. The government is used to approaching security, the same way I'm used to from years in the Army and all the rest of that, as in health and security is its own function that's well understood as to why you do that. But when you're trying to present that to a board, they want to know dollars, not just costs but what that offsetting on. And we're running into some issues in the industry right now where we've got two of the sharpest companies in business are telling us, a single lost record is $154.58. I can't monetize that for my board. I don't have that kind of information.

And that's someplace else where the government could help, is to try and develop out, because when private corporations try to calculate that, they're going off the information that's available to them, and that's a much smaller set. If you really want to get corporate board buy-in to security, what I need is the government to come along and say, "We talked with a whole bunch of different companies and our estimation is a lost record is going to cost you $215," or something like that. It's something that lets me take that back to them.

CARLOS KIZZEE: Let me real quick riff off of that question for just a minute and ask the panel, you know, so we're talking about information sharing and analysis organizations, this executive order. How is what we are doing, under this new executive order, addressing this problem, you know, helping to make people more sensitive at the board level, and, and, and making the non-security person sensitive to the problem? How is what we're doing and what we're here to talk about addressing that particular problem?

BRIAN SCULLY: Well, just to go back a little bit, to try to answer both questions, I think there's, there's a couple of things to think about. So from a federal standpoint—and this is something we try to do regularly—we like, our leadership likes to talk to CEOs. It's just, it's, you know, it's just something they like to do. They're at an equivalent level. We try to organize those meetings regularly. But there are a lot of challenges with that from both sides, right? So the CEOs have limited time, there's a limited number of issues. They want actionable issues. I don't know how many CEOs would want to come in and have the Federal Government train them on how to understand intelligence. We do do a lot of threat briefings, when we send briefing teams out, meet with companies and corporations and things like that.

And so we—there's a lot more than can be done. We try to do it as best we can. It's not always successful. I think it's a two-way challenge. I think the other part of the challenge, though, is, is, you know, we can go out, and we can talk—and this is training, in general, right?—is you can train all you want but if you're not exercising it, if you're not using it regularly, if you're not kind of engaged in those sorts of activities on a regular basis, it's almost you have to be re-educated each time it comes through. And so, again, there's, there's things that the Federal Government can do. We do invite senior leadership from corporations to exercise with us, and we do share intelligence with them. We allow them to participate in decision-making processes. We try to, we try to put all those together, but it's not easy on either end. So it's a tough challenge but I think a lot of us are working towards it.

From an ISAO standpoint, I think depending on the level of engagement in the ISAOs, right, if you're getting C-level, if you're getting senior level leadership, board level leadership participating in the ISAOs, I think the, the nice thing about ISAOs is that there's a lot of flexibility, right? You know, depending on how the standards come out, and, and, and things like that, there's going to be a lot of flexibility in terms of how these are set up, how they're run, how they're managed. And so they can be tailored to meet the needs of whatever set of CEOs or industry officials or things like that, or whatever topic, whatever subject is of particular interest. Again, this is—you know, I'm not a cyber person. I'm more of a policy and physical

security side. But there's a lot of opportunity there, I think, in the flexibility of the way the ISAOs could be stood up to allow for this type of activity in a more meaningful way.

I'd say the third problem is just getting cleared space, out in the field, for CEOs to be briefed on such things. I'm sure our intel person may have some more thoughts on that, but that's it from a policy standpoint.

BRUCE BAKIS: I'd like to pivot a little bit off of that question, actually. It seems to have a number of dimensions to it. But sort of bringing up to the, really, the topic of the day, and from a practical perspective, Mick Costa really talked about the Advanced Cyber Security Center, and so we talk about information sharing, have lots of different dimensions—strategic, tactical, operational—and really down to the technical level.

One of the forums, a forum that was run recently by the Advanced Cyber Security Center, was hosted at the University of Mass in Lowell, and the topic was workforce development. Now, it's been written up on the, on the ACSC website, I'm sure. I'm not sure there's anything really that's, that's really actionable directly from that single, that single forum. But that's where members engaged on obviously a very strategic issue that affects everybody, and there was a lot of contribution because their universities were certainly critical and they were involved in this discussion. So that's the workforce development piece of it.

Then I think that is the topic of discussion in a number of ISAOs, and I just gave you a specific example. So it's not that there's a solution, but it's really part of a strategic conversation where people understand that's really—there's a critical need.

The second piece of it, or another piece, is where you're talking about forming basically an intelligence organization within, within your organization. MITRE has some practical experience there. We've—we haven't always been sort of world-class organization but we certainly are now. We've actually captured some of those experiences and that's available. It's "10 Strategies of a World-Class CSOC," basically. And that might help you and other organizations as they try to mature and create an intelligence-based approach.

The other piece we're talking a little bit about, sort of senior-level executive buy-in, and I think some place—and, of course, we all struggle with that—there's a substantial investment that we at MITRE have made on the order of many tens and tens, on the order of about 40 full-time equivalent staff devoted to the defense of MITRE's networks, and the reason for that is, you know, we're protecting some, some intellectual property, and we're safeguarding sensitive information on behalf of our government sponsors. There's a lot there. And plus we also leverage those experiences from our own first-hand defense, and we sort of use that to work with our government sponsors. So that's one of the reasons why we have such a large defense organization.

But the metrics piece—I mean, and so we have to justify that expense—so the metrics piece, we've actually externalized that. I think there's a, there was a public release piece on that. If

you can't find it then maybe we'll follow up afterwards and I'll grab a card and an e-mail, and I can get my hands on it and send it to you. It's a briefing where, where we focus on really the metrics that we discuss with our executives, and key to that is the notion of a bull's-eye with, essentially, the sensitive intellectual property in the middle, and we're letting our executives know how close to the center any one of the threats that we've addressed, how close it's been. And the good news has been that there isn't anybody that's been at the bull's-eye. But that's an interesting part of the conversation at an executive level, is they're interested in things like that. And that's all part of, how come there are so many guys? How well are they doing? So we've expressed that in terms of metrics that might be helpful.

CARLOS KIZZEE: So in the interest of time, I wanted to open it up for one or two more questions, and there was a gentleman in the back that had a question. You're standing?

ATTENDEE: [Speaking off mic.]

CARLOS KIZZEE: So the trust model, the question. Who would like to tackle that?

MARIA VELLO: I think, you know, if you look at other like—companies that do similar things, maybe not for the retails but other, for retailers, but maybe for some other industry segment, you know, getting a group of people that you already have been working with, you've already established some relationships, you have some trust, and you start talking, because, you know, your software for service, I mean, you're going to have some of the same issues. You know, and if you can look at, you know, coding, you know, some of the, where are people trying to sabotage your code? Are they trying to counterfeit, you know, your software? I think you start sharing what's happening, what you're seeing, then you guys can help each other, you know, put up your defenses. Maybe you have seen something they haven't, and vice versa. You have to start small. You have to have a focus, you know, in a small group, and then start to build out, because I'll know somebody, and I've been friends with them, and I trust them, you know, and I've know them for, you know, 5, 6 years. I'm going to bring them into the group if you're adding value, if you're able to demonstrate results, you know, things that you can leverage, you know, in your tool kit to help you, you know, with your software and service.

CARLOS KIZZEE: I would add to that perspective that, you know, how broadly you share within your community is going to be a function of what I share with you, right? And so someone on the panel said earlier, it depends on who you are and what you're doing. So, you know, there's a bit of a function there, I would add.

There was another question right there, and I probably have time for one more up front.

ATTENDEE: [Speaking off mic.]

CARLOS KIZZEE: That's probably a good question for Mike. In the absence of Mike, I think the Bureau is probably the best person.

STACY L. STEVENS: Yeah. I mean, I would say that the way we partner, in that we don't turn anybody away. If somebody wants threat briefings, we try and be threat-based to see where we need to focus, based on an imminent threat that we're seeing or some sort of trend that we're seeing. So, an example of that is over the last couple of months we've been seeing a trend with folks, nation states, looking at personally identifiable information. So what we did was we brought in the health care sector into each one of our 56 field offices, and we had them get temporary clearances and provided them with that threat briefing.

So as far as the ISAOs are concerned, we did have some health care associations that I would proffer would probably be considered an ISAO as well, that were invited to attend. So I think that that's what we would do is probably leverage our field offices in order to reach out to and establish the partnerships. I'm not saying that we wouldn't do that at the headquarters level as well, but it would be more threat-based. But, yes, you would have the opportunities to, to meet with and be briefed on whatever information that we would have.

So I think it's a good opportunity. The ISAOs, the ISACs are a good opportunity to get a lot of folks briefed at one time, or leverage that ISAO to be able to push the information out to their members. So I think that that's a great benefit. That's how—one of the questions you had proffered was how do we work with ISACs, and I can say to you that we do have a robust information sharing process with the FS ISAC. We are engaged with them on exercises. We bring them in for our briefings. So that has, that partnership has grown where we leverage them to get information out to the rest of the members. So I think that's how that relationship with the ISAOs would be, similar to the ISACs.

CARLOS KIZZEE: So what I'm going to do now, standing between you and lunch, is a short, 30-second, last word from each of our panel members, and, Maria, I'd like to start with you and work your way towards me.

MARIA VELLO: Geez, I'll tell you. Okay. So I think, you know, as we look at what's transpiring and we look at today, I think one of the key things that I believe we should all do is take a step back. You know, let's not reinvent the wheel. Let's look at what's working, you know, how do we enhance, perhaps, what's working. You know, we cannot afford to have a fragmented approach to this problem. You know, if we take some lessons from our enemies' playbook, from these threat actors, they share everything—how-to documents, where we're vulnerable, how we're vulnerable. Today we're going to come out with a paper and we're going to publicize that paper all about what we talked about today, right? Guess who's going to read that?

When NIST announced, you know, that they, all the guidelines for NIST, in the underground forums, it was translated in multiple languages, and, you know, I will tell you, I was at a conference presenting and I said, "How many people know about NIST?" About 300 people, about 25 people raised their hands. They know what we're doing. We should take lessons from them. We shouldn't, you know, blog, tweet, talk, publish everything that we're doing. We shouldn't replicate, you know, or duplicate efforts. We should take a step back and take

some of the lessons learned from every one of the models and maybe combine it, and don't take a fragmented approach. We need a central repository for all this information. It can't be in multiple little pockets where nobody has access to it and nobody's putting all the pieces together.

So I think, you know, that that would be my closing thought, and I just want to answer one question. CEOs are more aware. You know, so I'll take one to digress, and I think focus on brand and reputation, focus on what's key to them, and that's more important to them than, you know, how much a record costs. It's what's it going to do to damage their reputation.

So, with that, I just want to say thank you to everybody.

STACY L. STEVENS: And I would echo Maria's comments. It seems like we have the, the same thought processes, maybe because we're both from Pittsburgh. But I just wanted to say that we do have to take a step back and look at this, because as these ISAOs form, we need to know why they're forming, what information we need, what information you need. So I know, you know, 2 years ago somebody said, "You're in charge of information sharing," and my first question was, "What information?" And so we talk about it constantly—information sharing, information sharing. Why are we doing it? It's going to be different for what you guys need and what we need. So we also have to have an understanding of, again, you know, what your, what your challenges are and what our challenges are for information sharing, and why we can only, you know, pass some information and not other information, and why you can only pass information, and, and certain information and not other information.

So we've got to kind of look at each other and see—get a better understanding of what we all do and why we're doing it, and what the limitations that we have in information sharing. So those are the two things, is figuring out what we need to share, why we need to share—and I'll add another one—and how we're going to do it. And go Steelers.

[Laughter.]

BRUCE BAKIS: I've got just a couple of sort of sound bite observations in terms of, as we mentioned, that we helped catalyze ISAO-like organizations across the country. And what we're seeing is, again, some difficulty in terms of overcoming inertia. So when people say, "Can you help me a little bit?" this is some of really what we're telling them in terms of how to get going. So first and foremost—and we did address this—you've got to be able to articulate the essence of who you are, and what you are, and what is your mission. And as easy at that sounds, it is very difficult for people to do.

The second piece—and we talked about this a lot today—is what are you going to share? Again, it's almost a little, sort of—you think it sounds easy but the ability to do that is sometimes really very difficult. So we're going to start with potentially, you know, indicators, but beyond that what are we going to share—TTPs? Best practices? You've got to be able to

articulate what it is you're going to share, and that really dovetails, obviously, with the mission of who you are and what you are.

Sort of the third piece of it is, we also—and this is really one of the questions that Carlos really asked, is what is the value proposition of, really, the ISAO, and, in particular, how are you differentiated from another ISAO, from an ISAC, and how, how do you fit in with the cyber ecosystem in the environment that you're operating within? One way to look at some ISAOs is they're a business. And so what I'm saying is really very consistent with if you're going to form a new business, these are the things that you have to tackle.

Another one of the, the sort of the areas that we asked people that they really need to focus on is, again, it's essence of, what's the criteria for membership? Who's in, who's out? Are you regional? Are you sector? Are you an affiliation group? You've got to be able to understand what are the, what are the attributes of a member that you want? You've got to be able to decide, like who's in and who's out.

Another one of the things that we tell people that they need to focus on is, again, this issue of trust, but now I'm thinking about it from a hub-and-spoke architecture, where—and Maria's talking about a centralized repository for information—who runs that? Who operates that? How do they safeguard that? How can that entity really be trusted? So we've got to think about the architecture of, really, who's protecting that information.

The next piece, the next item is—and we talked about this a lot—what is the role of government, in particular, on law enforcement? We've seen, in some of the consortia that we're working with that there is—people don't want the government fundamentally involved. They want it to be a closed group. In other organizations, they say "We want to share," and, in particular, that's really, that's an absolute requirement of the NCFTA. Law enforcement is embedded and involved. But we see that relationship elsewhere. People are—they, they're a little concerned about that. So you have to figure out, really, what is the role of the government.

And then, again, consistent with this notion of operating a little business—and we did have the question that was out here—what's it take to run this? What's the financial plan? People don't necessarily always think about that. There's a lot of sweat equity that goes into actually overcoming the inertia to form these, but you have to figure out what is the financial plan. How are we going to sustain ourselves? Is there a grant someplace to help get us bootstrapped or is it all sweat equity, and then how do we, as we, as we move on, how do we, how do we sustain ourselves? Is it through dues? Is it through licensing, potentially, of some intellectual property that might come out of the research, in particular, research consortium? So it's the financial plan.

And then, wrapping up, what's the fundamental sort of leadership and governance of the organization? Who's going to run it? How's it going to be run? And then, finally, what are really some of the high-level implementation milestones? You know, Mick Costa was, again,

talking about the, the Advanced Cyber Security Center, and he didn't have time to go through the history, but it was the twinkle in the eye of a number of people in 2008, to form the Advanced Cyber Security Center. It launched officially in 2011. So sometimes these things, without really an implementation plan, they can take a long time.

And so finally—and I said this initially—think big, start small, move quickly.

BRIAN SCULLY: Great. So I'll be super quick. My colleagues here covered most of the key points. I think the one thing I'd want to say is—and we've talked around this a bit and we've talked about it directly—that is information sharing is about networks. We are a network approach to information sharing, and so we need to think about it, the way we share as a network. Within that network we have both formal structures, ISACs, ISAOs, fusion centers, we have all sorts of operations centers, but we also have a lot of informal networks, right? When you have a question or you're hearing something, you pick up the phone and you call a colleague, you go to your Rolodex.

So the question for me, that I've been kind of pondering as I've been working through the federal information sharing framework is, how do we bring those two, informal and formal, networks together in a way that can strengthen our overall network, our overall ability to share information across the nation, to help us become safer and more secure? So that, to me, is there's a role for ISAOs in that. There's a role for ISAOs to bring together both the information and formal networks that already exist, in a way, and bring them together, strengthen the overall network, so that we can do a better job of sharing information across the board.

Right we have, you know, there's some pockets, there's a lot of informal networks. When a challenge arises we reach out to the people we know. We build trust that way. So how can we use the ISAOs to expand those trust networks? How can we use ISAOs to build the overall network and strengthen it? You know, there's all sorts of network theory out there and social network theory on how to do that, but for me that's the question I've been pondering the last couple of months, and I think the ISAOs can play a huge role in really strengthening the overall information sharing networks that exist. So I'll end with that and let you all go out to lunch.

ROMAN DANYLIW: Before you go out to lunch I'd really like to thank each and every one of you, and Carlos.

[Applause.]

ROMAN DANYLIW: This really got the conversation going and seeded things for this afternoon, which is actually going to be all discussion for us, no presentations, no further panelists. So, logistically, we have until 1:15. If you'd like to come back and participate in Breakout Session 1 and 2, we'll be in Room 120.

Thanks again to the panelists.

[Applause.]

Track 2: Analysis—Capabilities

ATTENDEE: Welcome back, everyone. This is the Analysis Panel. I introduced David Mussington. He is from IDA, and he's going to moderate.

DR. DAVID MUSSINGTON: Okay. Thank you. I'm David Mussington. I'm from the Institute for Defense Analysis in Alexandria, Virginia, and we support, like some other FFRDCs do, DHS and other entities who are working actively in this, in this arena, about the information sharing and operations and analysis and OT&E, and in some other things through our support to the National Security Agency.

I had one plan for this panel this morning, but unfortunately that plan collided with the discussions we had this morning. So I think it's fair to summarize an earlier session by saying that there might be more—less agreement on more things than maybe was anticipated by some other people, so what I think we need to do is begin by trying to capture experienced subject matter experts who have some insights on what they think is currently working, in terms of information sharing and analysis, because analysis is being undertaken for critical infrastructure cyber security currently. And a good place to start for future requirements and for future performance-based standards, perhaps, might be an analysis of what's working well right now and what future challenges might be.

So with that, that's sort of what we're going to do this afternoon, so I'm going to begin by asking each of the individuals to introduce themselves, and then we'll basically go serially, trying to—again, having our panelists comment on what, what analytical processes or methodologies they feel are currently working well, or at least are promising, and what challenges they think an ISAO might have to meet in advancing those capabilities, or in creating new ones, if the ones that exist currently look like they are of limited future utility.

So if I could start with Ken Stoni as our first speaker.

KEN STONI: Oh, sure. Well, thank you. First I'd like to start off by saying thank you to Mike Echols and his team at DHS for inviting me here today. It's a pleasure and an honor to be here.

So my, just a bit about my background, I, I'm with a company called ESRI. We are a software company that does geospatial information systems, so the software that provides capability to do mapping—kind of an unusual fit for a cyber guy. So before that—I've been with the company for about 2 years. Prior to that I was a U.S. Air Force officer, so I was a cyber planner and strategist throughout my career, for 21 years, but most recently at NORTHCOM and NORAD, and I had the same position down in Special Operations Command. Okay. So based on that experience, really looked at cyber as more of a cultural issue. I mean, there's a lot of technology involved, but when it got to coming up to a planning at a COCOM level, and, and developing strategy, you really can't fight—well, you don't want to fight data point by data

point, right? So the idea is to take all the data from all these different realms, integrate it, be able to put it in front of the commander as a campaign, and then start fighting the trends. Right?

So that was really the key. Data integration was important—which is really what drove me to mapping. So when you're trying to get an Air Force officer and a Naval officer and a cyber warfare person and an IT person to talk together, the lowest common denominator is really mapping, right? You really have to get to the point where there's a common model, a common understanding, and then discuss deviations from there. That also happens to be kind of the output of the COCOM, is to, to look at all elements of national power and apply it to problems that you face, right? So when you get to applying law enforcement capabilities or military capabilities or diplomatic, that's also geospatially bound as well, right? So it was kind of a nice fit to be able to, to get cyber, to put it onto a map, to get people to understand it, and then be able to kind of start brainstorming on how we react. You know, how could other operations support cyber, how could cyber support other operations. So that's what really drove me into geospatial.

Preparing for this meeting I kind of went back and, and looked at the last meeting, and there's a couple of points I thought I'd make a comment on before getting into the, the opportunities and challenges. I was really kind of interested and happy to see a lot of emphasis last time on information being a means to an end, right, although at the time they said the end was situational awareness. I think I'd propose that really situation awareness is also a means to an end. Really what you have to get to, I think, is consequence analysis, being able to understand what cyber disturbances, or what physical disturbances, what the consequences will be, because that forms a basis for resource prioritization, and I think that's the key to being actionable.

We've heard "actionable" quite a few times already, and the idea really is you want the organization to, to see something, to see that it's important, important enough that you dedicate resources to it because there's never going to be enough resources to harden all your devices, right, or respond to every alarm that you get. It's really just inundating. And, in fact, most of the organizations I worked with, no matter how large, really kind of suffer from data overload and information scarcity. So if you were to define information as the opposite of uncertainty, we end up collecting data over and over again, right, and there's a cost associated with that. There's a cost in collecting it and storing it and analyzing it. So if you're collecting repetitive data and it's not changing the way you behave, it's kind of a self-defeating process in that case.

So the really important part is to get to resource prioritization, to be able to integrate that so you can talk to different disciplines, right? So when you go to—at least within the Department of Defense—when you go for resources you're going to go in front of the commander, and it's always tough for IT or cyber folks to go in front of the commander and say, "You really need more X rather than another airplane," right, or rather than another ground, ground unit. So you've got to get that—you've got to get it right, got to get it into, you know, a format that they

can understand, and then we have to really kind of focus what we're looking for. So, once again, the data—it's not just about data. It's about catalyst data, for lack of a better word, right? In the military we call it the golden BB. I guess law enforcement calls is the smoking gun, right, and we see that when we find those things, data sharing and collaboration works really, really well, right?

So if you read the Verizon data breach investigation report back in 2013, it said about 70 percent of organizations learn of a breach from outside, okay? So that means somebody is calling up the organization and saying that the data is already out, okay. When that happens, resources start to flow, companies get called in, things start to happen, right, and I think the question for the ISAOs is how do you get that same response before something bad happens. What's that data that you need that's catalytic to being able to get the organization to see the importance and to respond correctly? So if I were trying to frame the issue a little bit, I think I'd frame in those—that, that's the target, to, to identify and get that data.

This morning I was really happy to see General Touhill say neighborhood watch, because that showed up again, again in my notes, as I was taking, I was doing the research, and I was really worried about kind of offending anybody if I said that, but since the general said it I guess we're, we're in good shape.

But, really, that's what came to me is, is you can get all this, this threat data, globally important. You know, it's kind of like watching CNN, right? You can get the weather anywhere in the world but the threat is really locally, right? So if you start looking at having to identify anomalous behavior of an adaptive enemy, you really need a local understanding to see what's different, to be able to talk about it, understand it, and be able to respond to it, okay, and I think that's the way it's going, and that neighborhood watch metaphor fits really well, right? The neighborhood watch doesn't have to know what's going on in everybody's house, right? They have to know, kind of get overlapping perspectives of what's happening in the neighborhood, and they have to know when to call the authorities, right? So if you're looking at a prioritization perspective, you're collecting that data, you're understanding what's important, you prioritize your own response, but you could also help prioritizing governmental authorities as well, right? If something important, they need to focus on that, then that's something to, to bring up.

At risk of overplaying the metaphor, the question really becomes what's the neighborhood, right? So in geospatial terms, the neighborhood is kind of a shared space. Just as a suggestion—and I'd be happy to talk about it—you could almost look at cyber as source and destination pairs, right? So you're collecting data from whatever means, you get source and destination. Anything you can see continuously is probably the neighborhood for your environment, and it becomes a pretty interesting kind of discussion point, I think. So if you, if you're in that organization, you look at one facility. Some place might—and I'll just talk geospatially, because that's my familiarity—some place might show up that's unusual. You don't have an office there but you have a spike in your IDS alerting or you have some kind of net flow data that's going there that's unusual. If it's just one building, no big deal. If that one location is hitting all your buildings, you might be a little bit more nervous, right? If you find out

that all the buildings being hit, they're only hitting offices dealing with your intellectual property, you're probably on the verge of calling it an attack, right? Your response would be much different. The cyber data didn't change. The way you're looking at it didn't really change. You're just framing it a little bit differently.

So if we look at expanding that, if you had an ISAO that looked at an organization and defined a neighborhood, or even an ISAC, right, how it defines a neighborhood, now you're comparing those destination locations. If you find a location that's hitting all members of an ISAC, that probably becomes even more troubling, right, and as the ISAC starts—or the ISAOs start putting their data together, and you start seeing locations in geophysical space, or you could do it in, in logical space as well, that are hitting everybody, that becomes a national effort, right? So I think what the general put forward works, right? It scales from a local responsive level and it aggregates up very, very quickly to help identify, as a community, where we're worried about what's important and where we have to go. So it might be—I just offer it up as a way to maybe start aligning the prioritization of an organization at all tiers.

So I think the discussion this morning was interesting. We started talking about how ISAO's going into what's the analytics that work. I think one of the things that—the way I'm looking at it—is if you identified your analytical process, the target is to kind of find that, that catalyst data within your neighborhood. I mean, that's what we're looking for. If there's analytical processes that you could put out, you could, you could think of a series of functions, starting from maybe data aggregation, to data quality control, to filtering, to modeling, to alerting, to response activity, as a single process but with multiple outputs, right? Your ISAO might only want you to aggregate. They do all the rest of it themselves, right? So it's one common process. They're going to jump in and out, your, your members, at different stages, and you would deliver to that membership, right? There's no reason necessarily to provide everything to everyone. But those standards can write the whole process and your users can jump in and jump out as they need to.

I've seen bits and pieces of this working very, very well, so it's really hard to say, universally, what would be good or not. I think that would be a start. I think we're probably in kind of an exploration phase where we're going to put this out, we're going to collect data, we're going to see what works, and maybe that's the way to start.

The challenges? I mean, I think we're still early. We're still in the exploratory phase**.** I think both the benefits and the challenges will kind of show themselves. I think the thing really about trust and—and it's kind of a, kind of a Catch-22, right? Trust—the more you have it, the less you have to prove it, right? So when you have no trust there's going to be a lot of data that has to be shared. When you trust somebody, you trust their quality, you trust their handling of it, there's less you really have to talk about, so things get easier. So I think there's that hump there. It's, it's a, it's a touch-and-feel kind of situation, and we'll see where it goes from there.

So I look forward to the conversation and thank you again for the invitation.

DR. DAVID MUSSINGTON: Thank you. You're staking out a couple of points—before I move on to Evan. Trust is probably a challenge that I'd like each of you to comment on. Trust and privacy concerns, and trust of government versus trust of private sector entities is probably an issue that's going to, to frame how ISAOs form through time. The notion of what constitutes the local neighborhood goes to whether it's a sector or a community of interest, or some other pairing, or, or triplet, or some, some other sort of set of actors that go here into a group. And the notion of triggers, for going beyond general awareness. So if, you know, when, when is trouble detected that elicits action? These are just some questions to help frame partner remarks.

So, Evan, go ahead please.

EVAN WOLFF: Thank you, and like everyone else I want to thank all the people that put it on, especially everyone in government service. Having, having been, been at the Department of Homeland Security for the first 5 years, which is like dog years, so that's like 30 years of federal service, so the—for others, I really appreciate everything that, that those who have served are doing.

I'm a—I guess I have a few hats here today. I'm a partner and co-chair of the data security and privacy practice at Crowell & Moring, which is an international law firm. I'm also a managing director at the Chertoff Group, and, more importantly, I'm counsel to the Interstate National Gas Association of America, which many of you may now be scratching your head on why INGAA is a relevant organization. But, actually, they are a small group of organizations that control the majority of our, our, our natural gas pipeline, distribution and storage, and, as you all know, to anyone who has had a cold winter, natural gas storage and distribution is kind of an important issue. And, and what they—they've come together over the last year with, with some good lawyering added in there, and, and built an actual information sharing organization. They've actually gone through and developed some guidelines on how to implement the NIST Cybersecurity Framework.

And so it's, it's been an interesting sort of learning opportunity, for which I feel like I, I was somewhat prepared for as a client, because my background, actually, before I was a lawyer, I have a—I worked in encryption analytics and numerical modeling. I was fortunate enough to be, to, to be a part of the MITRE Corporation with PUD 63 was, was passed, and we had to start standing up ISACs at the, the front end of, of this problem, and, and got to work for the government as a scientist for a while. So I guess I have sort of a, a, a geek and wonk perspective on this, and I speak Klingon and Romulan at the same time. So excuse me if I start ambling a little. I have friends in the back that will throw things at me.

To the point of what's, what's working, I think, you know, I would argue what works most right now is I think largely ISAOs are faith-based initiatives, and, and I, and while you can all think that's sort of a, a horrific statement for a lawyer to be saying in front of a large, off-the-record room, I, I think actually, you know, the sort of lack of clarity, the lack of certainty, but the amount of faith people have in this effort actually is really helping us do a lot, to make a lot of

motion, take a lot of steps that we normally would not get done, meaning that, you know, I am getting lawyers to, you know, lawyers, not outside counsel, but actual lawyers that are responsible for protecting companies' assets and information, to agree to share information without there being any regulations, without there being any real, you know, triggers.

But they're doing it because, first of all, you know, there, there, there is this desire to be a part of this effort. They realize there's some common good out of it, and this is where, you know, I hate cyber by analogy but there is sort of a, a faith-based initiative to, to what's going on right now. I think I, I will point—and I'm not going to—I'm not as rich as General Touhill so I'm not going to bet $2 but I'll, I'll bet a cheap cup of coffee at my, my free coffeemaker that, that I think that's not going to last. Eventually lawyers will sort of revert back to what we do best, which is be risk-adverse and say, "Wait. If we're sharing information, where, where is the liability of that?"

We're already starting to see that in, in some of the cases that are coming out of, of, of the other agencies, like the Federal Trade Commission, which has a set of these 50 unfairness cases and they're all really along the same idea that, that companies need to protect their data or else it's an unfair business practice, and, and that's causing, you know, some of this sort of retraction. I think we're going to, we're going to see that coming out of some large data breaches as well. So we're not always going to sort of have, have this sort of great opportunity. Similar to what happened at, you know, I guess during World War II, and what we experienced at the start of DHS, in, in that people were willing to help out because it was the right thing to do, and also people saw that it was a way of, of not only protecting our, our great democracy but the companies that, that, that are participating in it.

I do think there—another sort of point that's working well is, is this convergence of government and industry. I mean, the fact that we're actually able to have these meetings and people show up and we all listen to each other, I think is another sort of thing that's going well, and that, and that there is largely, I would argue, because of the, the lack of, of, of clear rules and laws that, that people can come together and, and talk more than, than they have in the past. And I think the, you know, the, the, what—my third point of why it's going well and then I'll start off with my list of 25 things of why it's not working—is because, you know, there is this sort of desire and, and—within, within the board room, and, and also within the sort of operations centers and companies to do something, and this is a very sort of easy and digestible first step. I mean, there are other first steps that people don't like, and I'm, you know, when, when we think about sort of where encryption technology has come in America, from, you know, the regulatory ITAR provisions to where we are now, we could see some very uncomfortable path forward that we don't want to take.

Just to, to, to be brief, some of the, I think, challenges that, that we face are, you know, first of all, this governance problem. We saw this earlier today. I was glad that, as a former MITRE employee, that we had a MITRE employee sitting between the FBI and DHS. But there's a governance problem and, and that was no sort of fisticuffs between the federal agencies on, on the, on the, on this panel. But I think there is a governance problem within industry, and, and

within government, and that we really don't know. I still am a little unclear when it comes to ISAOs what is DHS's role versus what is FBI's role. Sorry, Mike and others, if you guys have a very clear vision of it, but I spend a lot of time working with both agencies and, and I know how to cherry-pick, and when you go to the sort of third rail of the Secret Service, but I think that, that, that, that governance problem is also seen in industry, where companies are increasingly becoming more aware of how to manage this problem, and this is what, I guess, economists call a classic, you know, externality and companies are figuring out how to internalize it or developing mechanisms to internalize it, like environmental health and safety and other, Sarbanes-Oxley, and other areas of risk. But we're still, we're still at the beginning of, of that, of that growth, growth curve.

I think, you know, one of the more important challenges that we have, and it was talked about earlier, is metric. Something that when we were standing at bar—and I've been involved in now three—since I left DHS and MITRE I've been involved in three sort of ISAC, ISAO stand-ups over the last 5 year—and each one, you know, the business people have come in the room and said, "So how do we know if this works?" especially if you don't do cyber for a living. If you're an energy company, if you're a transportation company and your job is to move people or move goods, then cyber enables that, but you don't make any money off cyber. It just costs you, hopefully, less or more, depending on what, what sort of part of that line you're, you're, you're standing on.

And so I, I think the, the, you know, that, that's, that's a challenge, and, and, and another, I think challenge long-term is going to be the sort of where the law comes and maybe some—I'm the lawyer here so I'll try to be a little argumentative, or at least argue with myself—that, that I think laws really, in creating a regulatory environment for information sharing, you know, will initially sort of create some, I think, benefit. I think we'll see out of CISA, or whatever the, the, whatever the information sharing laws, the, the bills that we see coming out of, out of Senate and Congress, I think they're going to, they're going to initially help companies because they will create that liability. They'll create that initial protection.

But we, what they aren't doing is thinking about the entire lifecycle of information sharing, which goes not just from what you do to how do you get a signature from someone else's Snort box and put it on your Snort box, but how do you actually conduct a thorough investigation? How do you do joint defense investigations when you have common enemies and you have to work with multiple law enforcement agencies or, or the other big L word, which is litigation, and how do you do sort of joint litigation, which is really hard. I've been involved in three large data breaches that have, that have had six or more class action cases associated with them, and, and it was really hard representing a single company with a bunch of components, and if we had to have multiple companies involved—and this gets to be that sort of, that, that 3,000 figure that, that people bounce around, that 3,000 of these notifications happen externally—well, you know, for a lawyer that creates a lot of risk. And I think until we understand how to build a legal platform that, that provides the assurance that protects a company, that's going to be a challenge.

And so, I guess, just to, to be clear, I'm not saying that the current proposals, legislative proposals that are, that are out there right now—and especially one that, that has cleared the, the Congress—are not good efforts. I think they're great and I think they'll take us the next step forward. But I don't think those are—I mean, 3 years from now, when we're all together, I think we're going to be looking at sort of a whole nother level of, of legal and regulatory, and really business risk.

DR. DAVID MUSSINGTON: Thanks. There are a couple of terms that, that seem prominent in Evan's remarks. Metrics, which is something we worry about a lot, in terms of mission assurance against cyber risks, and that approve, prove the value proposition for whatever protections that you, that you want to suggest are important. I hadn't heard the term "the joint litigation" being identified before with a particular problem, but that sounds, sounds significant and not something that I've seen much literature on. Governance. Governance in terms of the SO, governance in terms of ISAOs, governance in terms of DHS and other agencies' relationships with the changing environment of information sharing actors, were all sort of mentioned as prominent challenges which we're going to have to deal with, successfully or not, but they will be challenges.

So, Joe?

JOSEPH VIENS: Sure. Thank you, and, Mike, Mr. Echols, I appreciate your inviting me to this pane and I very much appreciate being with the distinguished moderator and fellow panelists. Real quick, I think it's important for me to describe our ISAC. It's probably the most unique one out there. We are the official ISAC for the communications sectors, actually the National Coordinating Center through DHS, which is a subset of the NCCIC, and we heard about that this morning. We have 67 members of the communication ISAC. They range from network service providers, ISPs, to associations, to equipment vendors. The key requirement to be a member of our ISAC is to have a tie to the communication sector.

We come together every week with our DHS partners, with the NCC. We also recently, within the last probably year and a half, have developed a network service provider group subset of the industry side of the NCC Comm-ISAC—that's what we call it—and that group also comes together on a weekly basis, and we work collaboratively and we'll, you know, any member of that group can, can bring things up, certainly with, with our government partners in that meeting, and then also additionally with, with just the members.

We've had a long history of collaboration in the communications sector, dating back, really, to the Cuban Missile Crisis back in the early '60s, when President Kennedy was faced with the possibility of, of, you know, continuity of government issues and continuity of communication issues. So that was extremely important. In the, in the early '80s, President Reagan also felt that this was extremely important too. So we, we ended up having embedded reps from the telecommunication companies with, with government. So, really, we've been doing this directly for 30-some years, since the early '80s, and then more formalized in our ISAC with the PDD 63 effort, like the other ISACs as well.

So I wanted to give you that background. I also wanted to give you a quick background on me. I'm the Director of Enterprise Business Continuity and Crisis Management for Time Warner Cable, and we are volunteer—we have volunteer leadership process within our ISAC and we're elected to 2-year terms. And I only tell you that because I am not the cyber expert here, and I'm certainly willing to, to maybe provide some insight into how we may go about, you know, information sharing and some of the issues that we have around that. We had—the ISAC industry chairs submitted comments initially. I think that might be out on the ISAO website. So you can get more background on kind of where, where we stand with this.

But you talked about trust and privacy concerns. That's at the forefront of everything we do, because if we don't have that in place with our customers, it's a serious issue for us, not only from a business perspective but certainly from a regulatory and, and, you know, breach of, of legal, you know, ECPA and other data privacy laws that we are required by law to adhere to. So, you know, there are also antitrust issues that we have to be concerned with. We make sure that we adhere to all of those as well, as we interact with one another when it comes to this space.

So those, those are some of the challenges with respect to that. The legislation, I think, addresses that to an extent, and it's something that we are constantly working on to make sure that we do, that we're involved with, and make sure that it makes sense.

You know, some of the things that, that we really need to focus on as it relates to ISAOs is to make sure that they're, they're at high level and very general in scope, because every entity is different. Every entity's risk posture is different, and it's extremely important to, to make sure that you, you understand that, and, and to be too prescriptive with an ISAO standard, I think, could be counterintuitive to this initiative and actually do more harm than good. So I think we have to be very, very, very careful about, in this process, of being too prescriptive. Automotive information sharing. We talked a lot about STIX and TAXII this morning, you know. So if an entity, an ISAO doesn't have the ability—or even a big company, for that matter—have the ability to do that, does that preclude them from the process here, and, again, does that create, you know, more harm than good from what, what we're trying to accomplish here?

You know, we have to—we definitely—and I don't want to get into too much policy because that's not my, my background either, so I will, I will leave that to, to those that are more astute in that. But it has to be general to cover all, all, all sectors, and be flexible and enable, you know, their implementation across, you know, the diverse communities and disciplines. Definitely need to consider all existing laws. As I mentioned earlier, the data privacy that prohibit the sharing of, of personal data, so PII. We have to be very, very cognizant of that and careful of it.

I don't know if I, I strayed too far from your, what you were asking me to talk about. You know, the NCC Watch, in conjunction with the NCCIC, US-CERT, ICS-CERT provides a lot of our indicators and information around cyber security issues, so we are benefactors of that, as well

as government agencies and other sectors, for sure, that are involved. The companies within the communications sector do a very, very good job of protecting the networks. Obviously, we've got—if you look at it in, in three buckets, you've got our customers, you've got our enterprise, and then you've got our, our, our core backbone network. So those are the things that we're concerned with as it relates to cyber security. And we—I think, for the most part, our sector's done a great job of covering all of that making sure that we're leaning forward as it relates to protecting our, our, our entities and our customers, and all of our stakeholders.

DR. DAVID MUSSINGTON: Before I go to questions, just one point, I guess. You mention STIX and TAXII as being something that, that might impede cooperation if companies don't have it. I'm wondering, is there a standard that's, that's different in the communications sector?

JOSEPH VIENS: In terms of automated sharing, just generally speaking, you would have to have the ability to receive automated information, and what I'm saying is not all entities would have the ability to put forth that effort and the infrastructure behind it, in order to do it effectively.

DR. DAVID MUSSINGTON: So entities would probably like assistance.

JOSEPH VIENS: Potentially.

EVAN WOLFF: Yeah, I mean I guess here we have to sort of have the conversation about the haves and the have-nots, because I completely agree that, you know, with everything that he said about the communications sector, and I think the, you know, the communications sector along with—since there are a lot of IT companies in the room and a lot of people that service IT companies and banks—you know, you guys all, I go into this category, or the haves. You do IT for a living or you at least have a reason to do IT for a living. If we go out to, you know, retail, and, and, and energy, you know, there is a different perspective, and I've heard this before, that while STIX and TAXII is, you know, you know, complicated, and we, you know, there's still argument of what the acronyms even mean, and, and there's only one company that's really licensed it, and, and it has weird acronyms.

But the, the, the reason why sort of I, I like it is sort of because it moves us out of this faith-based initiative—and just so you know, I'm not anti-faith in any way—but it creates some sort of very specific, practical, and, as a lawyer, repeatable, which is sort of the—you know, a standard that lawyers always want to think about, is, you know, if we set up a system, is it something that we can rely upon? Is it something that, that is used by others? Has it become an industry standard? There's actually a whole line of cases called Daubert, to those of you who have sleeping problems, that you can look at.

But, but, you know, and, and, and, which talked to the rules of evidence, and that's really where, why, I think, I, I, and I, I do push for sort of having standards. And I can look to some examples of where they've been very helpful to the digital community. If we look at the payment card industry, for example, how we created the PCI standards did involve a set of regulations, but really involved everyone coming together and coalescing around a set of

voluntary standards, and that's sort of how STIX and TAXII were, were created as well. You know, we all agreed on the Kill Chain is how we're being attacked; let's, let's look at how we can sort of reverse engineer, back-end-out a way of sharing information that could help us stop this known phenomenon.

And so I think, you know, it creates that sort of meaningful way of approaching it. I also agree—just, once again, because I, I, as my 9-year-old points out, I continually disagree with myself every morning before I drink coffee—that it creates a problem, because it really is hard for simple companies to, or for companies that don't do IT for a living, for them to implement it. And so this is where I'm not worried about that problem, because I have 100 faith in, in, in sort of our, our development and technology industry, and we're going to make it much easier. You know, we've gone from—when I look at my first system administration job in 1988, to, you know, what my 9-year-old son does now, which is far more complicated in terms of his impact but better tools—we're going to automate and we'll get better at these tools than we are now. We're not going to be using, sort of, CACTUS and, you know, in, in 5 years we'll be doing something else but not that.

DR. DAVID MUSSINGTON: Just one remark before I open it up to questions. A lot of research has shown that small- to medium-sized enterprises aren't well served by current ways of disseminating threat information. A lot of research has shown that small- to medium-sized businesses aren't well served by current information exchange or sharing mechanisms. So STIX and TAXII, I'm not sure if that's the issue. It wouldn't be for most. But there is an issue of whether, in fact, the supply side will ever catch up with the demand that doesn't articulate requirements clearly enough to actually be served.

ATTENDEE: I mean, my short answer is managed security services are going to solve that problem, that and some overlaying regulations like we're seeing coming out of DoD, with the Defense Federal Acquisition Rules or the DFARS Safeguarding Rule, where if requires companies to have a secure supply chain. I think, you know, companies have realized, with their payment card and, and, brand, card brands in the, in the, in, in the card industry and the payment industry that, you know, they also have to worry about their supply chain. So I'm actually not worried about—my brother's a doctor and he has, you know, 50 employees, and he's never going to use STIX or TAXII, nor will he know what they are. But we do go to secure cloud providers to store all his HIPAA data, and, and so I think that's—I think the market—I have faith that the market will take care of some of that problem, or hopefully most of it.

DR. DAVID MUSSINGTON: So on that very sanguine comment—comments from the audience? Sir. We've got a microphone right here.

ATTENDEE: So to sort of play devil's advocate there, so for a small law firm or a small doctor's office, I can definitely see some cloud options for them there, but if you're like a very small 1-, 2-person retailer, or a pizza shop, or even just somebody who is just starting their practice, and there were regulatory requirements for you to go and meet these requirements, the only way you could do it was by going to a third-party security cloud vendor, that's not in the budget for

them now. How is that going to be in the budget for them then, in the future, when it's a requirement?

ATTENDEE: A small pizza shop still has to comply with OSHA, with workforce safety rules. They have to comply with a lot of other complex regulatory issues that they do through a variety of tools—and just to be clear, I'm not saying we need to start regulating small businesses for data security, but they, you know, they, there are, over time, they will, I think, develop a market, will develop a set of tools, just like, you know, GoDaddy allows, you know, someone with a, you know, a 10-year-old to be able to create their own website, without having to, you know, have command knowledge of, of, of, of how, how, what domains work. I think, you know, those, those same companies that are pushed to go, to go online will be able to go online more securely. I actually think it's going to take us some time and I think it will be built in supply chain.

But I, I agree, the small, the small to medium businesses are going to be sort of—I mean, they're the tail of this problem. Since largely none of them are here today, I think they're clearly the, at least, you know, a huge part of the problem that, that they aren't represented.

ATTENDEE: So one of the things we're doing, and have done with the CSRIC, FCC CISRIC working group for effort—you can go online and look at that. I think it's a 400-some-page report. We took that head-on, and we had a subgroup that looked at small and mid, mid-sized businesses as it relates to what are some of the impediments to adopting the cyber security framework. So I think there's a lot of information there.

Some of the things that we're doing on the comm sector side is we're doing educational outreach. We've got, obviously, associations that represent the smalls and mids, and we're providing webinars and, and other information to help in that effort. And then I think the managed services has got to be the option for a lot of them, if they can't handle their, their security requirements in-house.

ATTENDEE: Okay. Great. So just, just to clarify and make sure I understand, your belief is that the cloud and managed security markets will scale down to these people who want to enter the enterprise space, or the business space, but it doesn't necessarily mean that there's going to be a raised barrier of entry for these such that these sectors will only see large companies being able to operate?

ATTENDEE: I think there's going to be a balance and I think, you know, when someone is entering the market they have very low risk, you know. The data they store, you know, assuming you're not, you know, your, your market entry isn't building a nuclear reactor, but I'm starting something that has a low risk sort of, sort of entry point. As the risk increases they're going to have more money to spend on better managed security services, better cloud offerings. So I think that sort of framework. I don't think, you know, someone who's starting a company tomorrow as a sole proprietor is going to be able to sort of instantly do everything

that mature companies are going to be able to do, but I think as risk increases, there will be sort of this matching or sort of matching of risk and security.

ATTENDEE: Got it. Thank you.

DR. DAVID MUSSINGTON: Just around on that point, you pointed out many services, companies providing perhaps analytic services to small- to medium-sized. Does that suggest that a standards organization needs to be, needs to articulate standards for products that managed services companies provide? For example, if there's a—if an IDS service is offered by a managed service provider to small- to medium-sized business—the chain of logic here—and the small businesses are sufficiently small and not expert, that they don't fully understand the products they're buying, does the standards organization, sort of from that situation, gain a responsibility to, in some sense, enrich or certify the services that are, that are vended, ostensibly suitable for small- to medium-sized business?

JOSEPH VIENS: It's probably a question for me. Again, I think we have to be careful about how prescriptive we get with this process, because, you know, each circumstance is different. Each business, again, is different, and their risk and their profiles are different. So further regulating managed service companies, I'm not sure is necessarily the answer.

DR. DAVID MUSSINGTON: I didn't say regulated.

JOSEPH VIENS: I know, but, but being too prescriptive with, with respect to the services they, they provide. I think they do a good job on their own by describing their services to a prospective client, and you can just go out onto their websites and, and look at those pretty clearly.

EVAN WOLFF: And sort of in support of that statement, too, you know, if we all are in agreement that we can't regulate our way out of this, there, there isn't like companies are going to just be developing untested products, because, ultimately, as we've seen with, you know, litigation like coming out of the Federal Trade Commission—which actually has picked up, I would argue, this exact problem—then, then it ends up in courts, or these administrative agencies are developing what the standards are, and we've seen many times with data breaches, where it's judges that decide what is the standard of care for a company protecting and storing data. So I don't think we have to say if we don't have regulations for everything then, you know, we're in the Wild Wild West. We still have, you know, a litigation system and ultimately Congress could decide it wants to actually do something, and create, create some laws around this too.

ATTENDEE: If they could actually do anything. I didn't say that out loud.

ATTENDEE: So the short answer is no.

[Laughter.]

ATTENDEE: Now for the explanation. Those products that mentioned—IDS, IPS—are already certified. I mean, that's why you have NIAP, common criteria, FIPS 140-2, NIST 800-131A, et cetera, et cetera, et cetera. So to add another certification is just a matter of how much more cost you want to add. No, I don't think that the small- and medium-sized businesses are going to go to managed service. It's too expensive. The OSHA regulations and everything else are already putting them out of business, so the question is how do you simplify security? I heard the panel talk about how STIX is working. It ain't working. DHS is on one version of STIX, which is a version behind where the standard is, so we have to back-port that to try to get it there. That's why it was moved to OASIS, so we can actually make it a real standard, because all of us in the IT industry are having a hard time using it.

Let's talk the truth here, because otherwise we're going to ask some standards organization to tell us how do to the business with the wrong premise, and I submit that the premise is incorrect. STIX/TAXII is the leading candidate to move forward. I think it's going to be better than MAEC or IODEF, or a few others. It has the capacity—excuse me—it has the capability to become the thing that we're coalescing around, because industry and governments globally understand that's a problem, and we're desperate for a mechanism, but it can't be something that we took a CSV file, put it in XML, and all of a sudden watch it explode ten times, and you can't handle it or eat it, because a small or medium business can't handle it, and neither can a large very well.

And that is where we are stuck. So we're trying to get our way through that. So the standards organization doesn't need to focus on that as to how to make that work better. It's a matter of what mechanisms are out there that we can operate and share, and how do we type forecast, or the type of organization we are, and where we're trying to go with that information, in an attribute of how reliable that information is from that kind of organization. That would help us. I say that from having started the IT ISEC in 2000, and organized response at first, and doing large-vendor exchanges, daily. So we get how to do that. I don't need an SO telling me how to share. I need the ability to share with better partners and stop creating more organization to dilute the effort.

Sorry for the soap box.

DR. DAVID MUSSINGTON: Mike, could you respond to, or sort of refine a little bit what you see the SO's core tasks as being?

MIKE ECHOLS: [Speaking off mic.]

ATTENDEE: I think you have a good basis with the National Council of ISACs and the existing highly functioning ISACs, to be able to provide a lot of the insight and answer these questions, and I think—I think those ISACs can serve in a kind of a leadership role or a mentorship role here to develop, to develop these standards, for sure. I think we should look to what's working instead of trying to fix something necessarily that isn't broke, so to speak.

ATTENDEE: There are three types of organizations that you really revolve around. There's readiness, basically your security. There's your instant response—how do you actually respond, and attack, et cetera, and then recover? And there's a security effort around that globally, about how to define the service of what that is. We're actually meeting next Sunday in Berlin, for this subject. The third part is the information sharing. How do we get it from one individual to their like-type group, or community of interest, and then how do you then get that out to everyone else as an early detection, early warning, so that you can go back and do your readiness and your response?

So realize there's three different elements here, and we're talking about information sharing like it's all of them. We haven't defined those other two aspects, and they go hand-in-hand with this problem-solving. Now try to enlarge the ISAO perspective. You have to know how it interacts in the ecosystem. It doesn't do everything.

DR. DAVID MUSSINGTON: Any other questions?

ATTENDEE: I'll just make one comment to that, Steven. I think that many of the, again, highly functioning ISACs already encompass all of those qualities, so, again, I think we can certainly bring some richness to this process, for sure.

MIKE ECHOLS: [Speaking off mic.]

ATTENDEE: Sure. Yeah.

ATTENDEE: So we can maintain our way of life.

ATTENDEE: I'm not arguing against this process. I'm here to support it, for sure, and I—believe me, I have the same company sending me a letter from two different entities that have lost my information or breached my information. So I guess I guess 4 years of protection from, for these two breaches. I don't know.

EVAN WOLFF: Two concurring.

ATTENDEE: Yeah, two concurring.

[Laughter.]

ATTENDEE: Thank you, Mr. Lawyer.

[Laughter.]

ATTENDEE: So I get—I understand the problem, and I think we all do. That's why we're here, for sure.

ATTENDEE: I do—I mean, I, I, I guess I'll go back to the one thing that I've learned at DHS about the sectors, is the only thing they have in common is they're all different, and I think that we do need to take that into consideration when we think about sort of learning from these, the ISACs, the smarter, older ISACs, that just because you understand the communication sector—no disrespect to the communication sector—doesn't mean you understand even how the energy sector uses the communication sector, because, you know, they still use radio wave towers, and they use fiber as backups to control liquid pipelines. And so, you know, we—and this is a sort of a problem that DHS had at the beginning and why we ended up with sector coordinating councils, not more ISACs, is that, you know, there needs to be sort of a very guttural understanding that, that each of these sectors really do think about life a little differently, they have a different business purpose, and they have different reliance on, on cyber. And I do agree that information sharing is small jars for some of them and bigger jars for others, because some of them are focused on other parts of the problem.

DR. DAVID MUSSINGTON: Someone down here.

PETE PAYSON: Hi. I'm Pete Payson with DHS I&A out of Connecticut, and my question is—I work at the Fusion Center and we have this National Network of Fusion Centers that are already in the communities, that have established rapports with federal, state, and local law enforcement, also private sector industry. And what do you envision their role is going to be as part of this program that you're initiating?

ATTENDEE: I don't know. That's maybe a Mr. Echols question.

ATTENDEE: [Speaking off mic.]

ATTENDEE: I mean, I'll—that's a very—I admire that question, because it's a, it, because, you know, this, this is, I think how I'll sort of reframe it in sort of a question I think we can all maybe start answering to get to that harder question, which is what is the role of government in information sharing? What is the role of the NCCIC if, if you are a small business or a large international energy company and you have, you know, detected something, either on your own or through some third-party notification, something on your network? You don't have necessarily a duty to disclose it to anyone if it doesn't involve PII or loss of HIPAA data.

You know, you don't have to go to the NCCIC unless you want to, you know, have sort of some patriotic duty. But, at the end of the day, if you, you know, have, you want to make this an insurable loss you're going to have to report it to someone. It might be the FBI. You might want to go to—I spend a lot of time dealing with local police departments on large cyber data breaches, to be honest, because they're an easier place to do your initial reporting, if you want actually get a police report that you can turn over to your insurance company. And so I think that's where the fusion centers are going to be very helpful in that sort of reporting piece.

Unfortunately, I think, you know, they're going to be a step behind figuring out what is the role of government in this really incident response and some of this information sharing problem. I, it's just, it's a really, it's a really hard, hard problem, because right now the laws and lawyers sometimes don't exactly sort of support the goals that, that we're talking about here.

I don't know if anyone wants to disagree with me.

ATTENDEE: Well, I look at the fusion center, too, as we have all the components represented along with protected security advisors, who could go out. We do get a lot of cyber reporting. I also report into the intelligence community with cyber incidents and other things. And so I think the role of the fusion centers could actually enhance this, to some degree, where the expertise and the network is already in place to share that information. With regard to governance, I know in Connecticut we have an executive board that's made up by members, and there are some private sector sitting on that, that executive board for governance. So there is a network in place. It's just, I think it could be utilized.

ATTENDEE: But the challenge is, like in, for, if we're looking at an incident, you know, you're already—once you make the determination that you've had lose PI, you're already going to have to notify 47 state attorneys general and/or other state officials. So, you know, it comes down to this question, the sort of most-written memo in any data breaches, you know, do you have a requirement to disclose this to anyone? If not, see Section 2, which is, is there any benefit you get from disclosing this? And I know we're already going to have to call the Connecticut AG, I think it's within 30 days of, of the loss of PII, I believe is what the Connecticut law states.

And so, you know, can we get companies to voluntarily go to the fusion centers? That's a—I think that's a good question.

ATTENDEE: Yeah I think—I'll make it simple. Turn it into a question and then we can add to all this. The real question is, how do the, the government fusion centers and cyber centers—because I'll throw the cyber centers into the mix, how do they all play in the ISAO world that we're trying to create? I mean, that really is the question that we need to, to refine the answer to. And, on that note, Pete wants to say something.

Yeah, we're almost done. We're done a quarter of?

ATTENDEE: I think what we're describing is a need for an interoperation between ISAOs. Mr. Echols, your comment about ISACs, you know what they do and they do verticals, you know, we need to think of that as—you know, the verticals, like the IT or comms or other sectors will tell you how the system operates. But when you get down to the fusion centers, et cetera, it's how they operate the systems. I know that's a play on words but stop and think about it. One is how does it traditionally work—you know, bits and bytes are going to be bits and bytes overall. How you do certain commands on a system are going to be pretty much the same. But how you're employing them to support a business, to transfer data, and how you're going to protect

are going to be unique to your situation, whether it's geographic, it has to do with a certain type of business, a subsector of a subsector, et cetera.

And that becomes important because now as you try to paint a picture, you're going to a difference, and here is where I submit the government has a role, and that is helping put context as things roll and move, because that gives the impetus for people to act. Notice I'm not asking for a regulatory stick. I'm asking for a "let me understand what is happening," because that is a larger and quicker motivator, because Congress passing a law, we'll always be behind where we are in responding to the threat, because a threat is going to evolve, the technology is going to evolve, and economic and business operations are going to evolve. And those change. So when we go back to Connecticut, that's where the problem is on the ground, not how the systems operate but now they operate the systems.

DR. DAVID MUSSINGTON: Okay. We are practically out of time, so unless I hear—okay.

ATTENDEE: So the financial services ISAC, in our experience, has been working wonderfully, and the information that we've been able to share, you know, between the, the entities that were in the financial services was timely, actionable, and relevant, especially during the Ababil, Al Qassam fighter brigade campaigns, and that was a big win for us, and within that ISAC. But one of the things that we keep running into is all of the information analysis that we get from law enforcement and from government tends not to be timely and tends to be so vague that it's not actionable. And so what are we going to be doing different with this initiative to remedy that in the future?

ATTENDEE: I guess I'll take a crack and release what I see.

ATTENDEE: [Speaking off mic.]

ATTENDEE: Yeah, no, no. Go for it.

ATTENDEE: So I think, you know, educating as far as what we can provide, a lot of times because of investigative restrictions, a lot of times we cannot provide more information because it's at a classified level. And in the first panel what we basically stated was a lot of times what we'll do is once that general information goes out we do provide, based on a sector or whether it be an ISAO or a region or whatever, bringing in folks and giving that classified, contextual information that kind of puts the pieces together for the private sector as to why the information that's coming out may seem dated or it may seem like, you know, it's not actionable. When you get the context behind it, that allows you to kind of figure out what's going on a lot better.

So that's kind of what we're trying to do. We've been doing it for the last couple of years, since my program started, is to get that contextual basis and information out to the private sector, and then be able to say, "If you see something, let us know." It's almost like a request for information back out to the private sector. So I don't know if that answers your question as far

as how are the formations of these organizations going to assist in that, but it might be an opportunity for us to leverage and get more information out to a wider variety or a wider audience, as far as contextually concerned.

ATTENDEE: Let me give you another perspective. One, this executive order was promoting private sector information sharing. So one of the things that we ended up doing, Peter, is we were trying to inspire—or stand up for information sharing across the private sector. Then you don't have to worry about the government, right? What happens after that, when the private sector starts sharing more information between, within themselves, the government, all those things that you're saying, we have to come to the table with facts that are information, better information. So you're aspiring—by sending this private sector information sharing up—somebody asked me, "What do we need to government for?" Well, that's something that the government will have to ask itself, right? So we're going to have to get better.

So I think this is one of those things like a ladder, you know. Private sector takes a step, the government takes a step.

ATTENDEE: I guess I have a little bit of a different perspective because I do, you know, if, if you sort of had two scenarios of Company A getting information from the government or Company A getting information from Company B, most of the time they'd probably rather get it from Company B. So I think sort of the first issue of this strengthening the peer-to-peer information sharing networks is, is going to be very helpful, and I think that could actually, you know, result in better protection of networks. I think this also will force the government to do something different, not sort of race to, you know, intercept more data to share with the private sector.

I guess your word is "context." My word is "mitigation" and helping companies, especially those that sort of are, are new to some of this incident response world, or that, you know, are, let's say in some of these other sectors—energy, non-business, energy, defense sectors—every time there's a government release and they have this mitigation section, to, to lawyers and to companies, oftentimes that's the best part of, of the alert to see, because it tells you what you need to do. It tells you if you follow these rules, if you follow these steps, then, then at least you have, you've met a standard and, and, and it's probably a standard that makes sense since oftentimes a lot of mitigations come, comes out of NSD and other places that, that actually are very helpful. And so I think it's going to cause the government to sort of play a different role in this information sharing rather than just try to compete with peer-to-peer information sharing models.

ATTENDEE: I'll make one quick comment on the government piece. I think the continued collaboration—you know, the financial ISAC is on the floor of the NCCIC, we're on the floor of the NCCIC—I think the continued collaboration and mutual understanding of what our issues are is, I think, already proven to be very effective and improved things from where, where they were not too long ago. So, I think there's hope to, to improve that process if we continue in, in the manner in which we've been, we've been working hard at this issue together.

ATTENDEE: [Speaking off mic.]

ATTENDEE: Yeah.

DR. DAVID MUSSINGTON: Okay. I think with that we're concluding this panel. Thank you all.

ATTENDEE: Thank you for having us.

[Applause.]

Track 3: Automated Indicator Sharing—Controls

ANTONIO SCURLOCK: Alrighty. We'd like to welcome you to one of the final panels of the day, and I appreciate everybody coming forward and bringing their special friends with them. That's why there's an empty seat between each one of you, right? I brought mine too and he's sitting right here.

That being said, this last panel is going to talk about automated indicator sharing, and we've had a couple of discussions earlier today, one to speak about requirements, and for those who can't see in this recording I actually have that in parens, because we don't really mean something that we're going to leverage against folks. What we're really talking about is if we want to do this information sharing piece in an automated fashion, and what might be the future of the information sharing analysis organizations, what would be the kind of things we would have to have an understanding of—roles, responsibilities, and so on and so forth. So we had a conversation about that.

So a couple of individuals have sat in those meetings and I'll do a brief description of them, and I'll start off with the most important person—me. My name is Antonio Scurlock. I work for Department of Homeland Security in the National Protection and Programs Directorate, in the Strategy, Policy, and Plans Office, and I also—I'm a co-lead for the Enhanced Situational Awareness Initiative, formerly known as the Comprehensive National Cybersecurity Initiative #5. Exhale. Roger.

That being said, I'd also like to introduce you to Ed White, on your far left over there, VP of Public Sector and GHE. As such, he is responsible for developing—Centripetal? Got it—Centripetal Networks' strategy for supporting the needs, policies affecting the Federal Government, critical infrastructure, health care communities, and he's a 25-year veteran of the short-haired—no, I'm just kidding—25-year veteran of the federal IT industry, and he started his career in public service—you know, you've got to appreciate that, right? Always giving—in intelligence community. Always giving. And he has held more leadership positions than I want to read off here, and actually some pretty cool stuff. You led somewhere at Microsoft? That's hot. That's my place. I'm a Microsoft fanboy. Every time I see that work I get riled up. That's pretty hot. Nothing against Apple but I'm a Microsoft fanboy.

Ms. Allison Bender, DHS OGC. Enough said. No, I'm just kidding. No, she really is OGC, and she's been doing quite a bit for us in dealing with the automated indicator sharing, Executive Orders 13636, 13691, and also PPD 21 work, right? Okay. Roger that. And she's been advising the NCCIC on a number of operational issues, including serving the primary attorney for the government's response to Heartbleed and the USIS background security clearance breach.

Do we want to talk to anybody else besides Allison? I'm just saying. Okay.

And last, but most assuredly not least, is Mark Davidson, and Mark has been pivotal in speaking to us in a couple of the other sessions. So he is the author and architect of TAXII—don't hold it against him. He's been admitting to it all day. That takes a lot of bravery—and an integral member of MITRE's STIX and TAXII team, lead cyber security engineer at MITRE, and he has a cutting edge R&D team focused on the nation's hardest cyber security challenges. His areas of expertise include threat sharing, cyber security, and software development.

So hopefully you guys have lots of hard-hitting, difficult-to-answer questions that we will take up at the next panel, and we're going to focus on just the ones I want to ask today. [Whistles.] Nobody caught that? That was hardcore.

So let me start off with saying a couple of things. In this morning's breakout session we talked about, like I said, participants. How do you play if you're an ISAO? Various roles. So that be a straight consumer of information from a particular sector, and then passed on that information to someone else. Or are you going to consume information and rinse that information and then produce unique pieces of information? Would you play in both roles, where you're always consuming and producing information that's enriched from your trusted community?

Are you going to actually offer up infrastructure to be shared with your community, and therefore provide some sort of shared capability for these kind of things? And then, would you be playing the role of a broker, you know, and for definitions we have a literally got all of them worked out. But in this particular case the ISAO would be working as a community entity would take into account both the government and the non-government entity and their sharing, looking at the best interests for both sides of the house, if you will.

Good discussion about that. Some of the equities we talked about was weighing, if you will, anonymity versus having confidence in the content and context of the information being shared. Machine speed in the context of the trust relationships between the machines themselves versus the inter-organizational flow of information, as well as the intra-organizational flow of information. One of the other pieces that I kind of want to have a good piece of discussion here is, while we are moving towards this machine speed piece, we want to do that, but, you know, the question I have initially for the panel is, do we still maintain manual inputs? Do we still take non-machine-speed inputs? Or, do we see that as—the relevance of that not being quite the same as that constant flow of those trusted machines, pumping, consuming, and producing information?

So I'll start off with that.

ED WHITE: I'll take it. To my opinion on that would be probably have to do both, because you have a different, a different scale of, of individual capability that's going to come across as the ISAO organizations grow. So initially, you might actually have to take the manual input and then transfer that manual input into something that's going to be more, obviously, efficient and effective, and your ultimate goal would be to get everybody the machine rates. Obviously you can have STIX some TAXII standard or something to that effect. You want to be able to, to, to collect that information dynamically, update that information when it changes, and be able to consume that information at line speed or you're going to find yourself not being able to keep up with the adversaries as they move forward.

ALLISON BENDER: I think Ed is exactly right that we do need to maintain the capability to ingest and disseminate indicators in a manual fashion, but at the same time as we're focusing on providing timely, relevant, and actionable information, we need to decrease the amount of human review that is required, increase the amount of automation that is available, both for intelligence analysis but in a way that also maintains privacy, civil liberty, and other compliance controls, really focusing on how we can do that moving forward and bring down the time from months to milliseconds, and how we'll be able to share information so that organizations can best protect their infrastructure.

MARK DAVIDSON: So apparently there's a solution or an answer to this question because I agree with the other two panelists. I think that both manual and automated means are absolutely necessary. I think in terms of accepting intelligence from a, from a broad diversity of potential inputters and producers—I don't know. I kind of tend to look at things within the technology realm and one of the axioms of implementing protocols is be generous in what you accept and be strict in what you send. And I think in following that it would, you know, allowing, really, a great variety of inputs into any indicator or threat intelligence sharing system or community that we might be developing, I think it lets anybody take the knowledge they have and put it into the system.

Now, I think that the automated mechanisms will ultimately be the more efficient, higher value way of doing it, but somewhere along the line there will be somebody who sees something and their best way of inputting it will be to just maybe go to a, a website and say, "Hey, I saw this; can you do something with it?" And then I think from there, you know, the entire subsystem can be automated, but it's going to be interfacing with humans, so the system needs to have interfaces that are comfortable for humans to use.

ANTONIO SCURLOCK: Roger that. I appreciate your answers on that. As a matter of fact, I'd be more than happy to take an answer from the audience if they have any feedback they'd like to offer on that particular piece.

[No audible response.]

ANTONIO SCURLOCK: Okay. Roger. We're going to move on to the next question, which may be harder, actually. So what you heard here, and this is what I gleaned from the answers, were—and what we actually talked about earlier was an economics of scale, that some organizations are going to be able to do considerably more than others, and even as you go into the ISAO, the ISEC model that's currently existing, whether you're sharing directly with the federal cyber sharing, like the NCCIC, one of the things that was shown—and I want to kind of have a discussion about the communities of trust piece—when General Touhill was giving his brief, there was a slide, and it showed the NCCIC, if you will, at the center of a hub-and-spoke type of information sharing, and I think what a lot of folks in the room that resonated as to that would be the only way, and the like.

And I'm not saying it is or it is not, but I'd love to hear the panel's opinions on the idea that, do you see that as the only way to go about doing the automated indicator sharing, or could one envision multiple hub-and-spokes that are interconnected, much like we do our networking today?

MARK DAVIDSON: So I think in terms of the multiple hub-and-spoke, I think that might be kind of part of what some people's vision is for the ISAOs. So it was mentioned earlier that there might be, over the next 3 years, maybe something like 200 different ISAOs, and each of those ISAOs is going to have their members. So you already, there, have a bunch of disparate hub-and-spoke kind of drawings, right, if you just think of the ISAO here and each of the individual organizations here. But then you're going to kind of have like a hub-and-spoke of hub-and-spokes, where each of the ISAOs maybe all connect up to DHS or some sort of, you know, getting indicators from the government or something like that.

So I think in terms of the—there's really maybe two different perspectives of it. There is the organizational architecture, which is each of the ISAOs and how they relate to the government and their constituents, and then in terms of automated indicator sharing, one of the ways that I look at it is the technical architecture behind all of it, and I think in terms of the technical architecture, hub-and-spoke is probably one of the ones that needs to be supported, but it should also be flexible enough to support the natural communication pathways that organizations develop.

ALLISON BENDER: So, you know, is there a way for entities to share information outside of the NCCIC essentially being the heliocentric point of all information sharing? I think that there is. I think that that is what happens now. Can the government help the private sector improve the way that they share information, whether that's through support for infrastructure or by providing, you know, policy overlays that support greater protection of privacy and civil liberties, other compliance controls? You know, I think that we can do that. In a lot of ways the ISAO models are a way of providing a lot of flexibility for how, how the private sector chooses to organize, and I will use my swimming pool analogy that I gave earlier. Especially because it's summer, I've been thinking about swimming pools a lot.

Information sharing can be like a swimming pool. Different groups have different requirements. In a sense, the NCCIC, being, you know, your local community swimming pool. It's government-supported, you sign your name on the way in, it's very light, easy to use, provides value, you enjoy your, you know, hot dog and cheap lounge chair, and maybe a cannonball in the deep end, right? It's great. Everybody's there and it's pretty easy to do.

There's all more sophisticated ways for mature users of being able to share information. In some ways this is more like the DHS CISCP program, the Cyber Information Sharing and Collaboration Program. There's an agreement to get in; it's the CRADA. It's kind of a heavy lift but it helps protect those trust community rules. There's expectations about membership. You know, there's not just the information sharing but there are these other activities. Maybe there's golf. Maybe there's tennis. But, you know, you also have to wear your coat and tie when you go to dinner at the club, right? You can go to the ATTEs. You are eligible to pursue, you know, conversations about potentially having security clearance and sitting on the NCCIC floor, being part of those more sophisticated, higher level collaborations. But it's an investment.

ISAOs, in some ways, can be like, you know, your neighbor's pool, your good buddy's pool. You can self-organize the invitation. It's still swimming. It's still information sharing, but there's a wide, there's a wide range of, you know, what that could look like. Is it, you know, a really luxurious pool with a hot tub, or is it, you know, a kiddie pool in the back yard? Do you have a lot of robust information sharing architecture that's, you know, supported and has all of the bells and whistles, or is it more of a light touch, manual exchange?

I think all of those things are possible. For the ISAO model, you know, it's up to you. Do you want to invite the government to your pool party? We'd love to be there. We think we can help, but it's up to you.

ED WHITE: I would add, basically, the, the one point that needs to be addressed, and I think Mark touched on it, is the ad hoc aspect of being able to share information bidirectionally, right? The importance of being able to do that is, is, is not lost on industry or anybody who's even sitting in this room, trying to consider being in an ISAO or being a ISAO, right? The sense of the, of, of being is what allows you to feel trust, and then that trust allows you to be able to share information more efficiently and effectively.

And if you want to get to an architecture discussion, which always ends up, since we're all in IT, I would say a federated approach on top of kind of what Mark already kind of described with respects to the multiple hub-and-spoke arrangement would be beneficial in the sense that you would be able to have a little bit more control of the DHS side of the house and more control at the aggregate ISAO. Rather than having some rogue guys running around doing whatever they want, maybe there's a way for us to be able to make this more controlled and effective based upon an architecture that allows you to be able to not only report and share but to be inclusive without being restrictive.

ANTONIO SCURLOCK: I appreciate your feedback on that. So, you know, it's interesting when we talk about the hub-and-spoke, federated processes, and at some point in time you start to look at the, the sheer scope, size, variety of the information and the entities that are sharing. And I'll get into some pieces, and tell me where you feel comfortable, talking about some of the architectures and infrastructure aspects of it. And from your view I'd like to have an understanding of, let's talk about the de-duping process, if you will, the ability to kind of score, if you need to, information that flows in, whether the infrastructure can handle all of that. Right now we have what's basically a, a push situation, or a subscribed situation. If we truly get into this machine, the machine, we might get into multiple avenues of query.

I know that was basically three-fold, but, you know, tackle whatever you feel like. But I think that as we go to this trusted, interconnected model, there's going to be some other avenues of thought that we need to take it to a place that, from a human standpoint, are easy. You know, the human sees the same piece of paper, and they go, "Oh, this is version 2. Version 1 is no longer relevant, because I can see that." There's a machine piece of that that needs to also plausibly happen.

MARK DAVIDSON: Sure. So I spend a lot of my day working on TAXII and other things like that, but I can speak a little bit to the process that the MITRE network defense team goes through. So basically what we like to do is we like to get indicators that are high quality, and what we do is we take the, the burden on ourselves of de-duplicating those indicators, and really any threat information that comes in. We have a, a threat intelligence analysis platform that we built ourselves and we open sourced, and I know there's a number of organizations out there that are leveraging ours. I know there's other organizations out there that have built similar platforms for themselves. And, really, the technology that we built, it has the ability to take in multiple things that are the same, and really all it does is it collapses them down into one entity and say I got it from these three different sources, or these four different sources. So you can track where you got it from, and partly in our information sharing efforts, that matters because where you got it from influences where you can send it to.

And right now a lot of our information sharing within MITRE is more of the ad hoc personal network-related, less automated variety. You know, as a member of the STIX and TAXII team I'm always looking for ways to get them to use STIX and TAXII and automate what they're doing. And then I guess I'll—so I'll tie that up and then quickly touch on another aspect. So at least for us, as an organization, we're completely comfortable de-duplicating indicators as they come in, at least at the volume we currently have. I can't speak to what would happen in a future increased volume state.

The other thing, though, is in terms of the indicator sharing ecosystem as a whole, what happens if it basically becomes a big echo chamber and you have maybe three indicators getting transmitted thousands of times across a variety of ISAOs and organizations. You know, maybe if there's a lot of organizations, I might be a member—you know, MITRE might be a member of three different ISAOs, and if you get some exponentially increasing number of the same indicator, I think that is just going to have poor implications for network health, and

hopefully, in terms of the system that we all designed, that's something that can be designed out.

ALLISON BENDER: Sure. I mean, certainly de-duplicating data is an incredibly important part of data quality, and when you're thinking about broadly further sharing this type of information you don't want to perpetuate information that is inaccurate, particularly if it contains information that shouldn't be there in the first place, like a certain PII, perhaps your proprietary information, other things like that. So, you know, the data quality process I think has to include, you know, some look at de-duping to prevent that echo chamber effect, but also applying technical mitigations, really a sanitization process, to understand the content, not just as you see it again, but is this content still right?

And then, lastly, you know, kind of thinking about how do we fix the echo chamber thing, one thing that DHS has been looking at very closely is using reputation scores to be able to identify like how good do we think this piece of information is. There's always going to be a balance between anonymizing your source and protecting trust community rules, and then for the entity that's receiving that indicator, do I trust this? I don't know who sent it, how did they do this analysis, and, you know, reputation scores are one way that we've identified that might potentially help alleviate that concern.

ED WHITE: You guys answered that pretty, pretty well. To add to that, I will, I will have to say, I don't necessarily think it's technical problem that we have with respects to de-duplication or architecture of whatever platform it might be. There are tools out there, like ours, for example, that can take 5 million indicators on every packet, right, and, and use those to, to make determinations on them. You have to be able to consume the information you need to consume, and you have to update that information that you need to update, dynamically, without losing the ability in which to make an indication, or an action on an indicator that you might be receiving.

So I think, technologically, we're probably ahead of the functional game here, and I think that's maybe what we all struggle with. We always want to throw an answer out there that says, "I have the silver bullet that's going to solve this problem," when really the problem is how do we put the process together, and the flow together, that allows us to put the technology in place to be efficient and effective to actually make these things work.

ANTONIO SCURLOCK: So, as I complained, I'll just quickly or briefly, when Allison got ahead of me on the PII, PCII discussion, actually, my next question was going to be your viewpoints on, well, okay, handling that type of information. I mean, do you let it come in? You ingest it. When you see it you chop it off, it falls to the cutting room floor and it slowly fizzles into the glass because it's acidic and you don't want to touch it? Is it something that you, you know, kind of induce maybe a compliance engine of some sort, that sees it and says, uh, maybe it's necessary to take care of the situation, or maybe it's not necessary? Your thoughts on that. We'll start with Ed.

ED WHITE: So we had a little bit of a heated debate in our last panel around—

ANTONIO SCURLOCK: It was heated?

ED WHITE: —what an indicator is. Is it an actual artifact or is it an IOC? And if it's going to be an artifact, which might include a PII-type of situation, there's a lot of things, as you just mentioned, that are going to have to be considered—as a consumer of that, as a user of that, as a provider of that, whatever stage you are in that ISAO type of organization. And I think that depending upon where you sit in that organizational structure, you're going to make those determinations based upon the risks that you're most comfortable with.

So we'll use the Joe's Pizza Shop analogy that we've been using for the last hour or two. If they're the ISAO for the community of interest of pizza stores, in, you know, Cambridge, Massachusetts, then the odds are he's not going to want to take in PII, right? He's going to say, "I'm going to cut that out, leave it on the floor, because that's too much of a risk." But if you were a larger organization, maybe the financial—like the financial ISAC, they might say, "I'm going to make an ISAO and I'm going to accept that information. Why? Because I need that information to actually create that transaction between those two parties that I have to help."

So it's really going to be dependent upon where you sit in that broader ISAO community, and in that chain as it, as actions have to happen, moving forward.

ALLISON BENDER: No, I think all of that is, is very much right. It depends on what you're getting, right? If you're getting unstructured data, you don't know what's in it, you know, unless you've done a manual review, and as we think about how to move from very manual, human resource-intensive processes to automated ones, you have to know what you're getting and what you expect to get. And I think with unstructured data, you, you typically get kind of two extreme reactions. "That's scary. Don't share it" is one reaction, and whether that's because there's personally identifiable information or potentially proprietary information, other types of sensitive data. I don't know what it is, that's scary, don't share it at all. And on the other hand, typically, from the cyber threat analysts and often from our law enforcement partners, they're like, you know, "I need it. Give me everything. I don't care what it is. I need all of it."

I think that there's a middle ground in between the two, which is to take a look at this unstructured data and either try and structure it or do some sort of analysis about what we're likely to get, what you should expect in, you know, whether it's an indicator, an artifact, and do the analysis at a more holistic level. At DHS, we do take personally identifiable information very seriously—civil rights, liberties, other compliance concerns—and protecting data is very important to us. That said, you know, even if it's PII, or potentially PII, we don't want to spend hours and hours redacting the bad guys' e-mail from a spear-phishing indicator, right? So for information that is necessary to understand the cyber threat, as a matter of policy we do not apply protections to that information that would otherwise be considered PII, right? We're not going to protect the bad guy. So what level of analysis is required to get from that unstructured

data to a high level of confidence about, this is what we expect to see, this is what we expect to be able to share. So I think that we're kind of in the process of moving towards that, but certainly I think it would be useful for other organizations, as they think about their information sharing relationships, you know, how is my data structured? Is it structured at all? How could I apply structures that would give me higher confidence in what I'm sharing, and then what sorts of technical mitigations or policy mitigations could you put in place to reduce risks in sharing information that has a compliance concern?

MARK DAVIDSON: So kind of I want to respond to two different things and then I'll say my own thing. So first, building on what Ed was asking, is it's basically what's the vision for the, for the ISAO framework that's going to be built? I think that's really the question that we all need to answer, and, you know, I personally don't have a great answer for that. But I think once you can define that vision and what it is, then I think it becomes easier to build out all of the things below it and all of the various factors and dimensions that we've all been discussing so far today.

And then, you know, you gave me a great platform to champion STIX out here. So STIX, the Structured Threat Information Expression. I know that some organizations out there—so once you have your, let's say it's an e-mail or something, and you decide that the, the recipient's e-mail address is something private, because it's, you know, a phishing e-mail that got sent to your company and you don't want your head of finance's information being out in the information that you share. You know, there's—once you have your information structured in STIX, because there's fields and it's structured, you can apply processing and say things. Like we always want to redact this field, we sometimes want to redact that field, in certain circumstances. So STIX enables that kind of processing to happen.

There's always edge cases where maybe somebody sticks an SSN in the body of an e-mail and that's more of a text search, but that's, that's kind of a different thing.

And then, I guess I folded in the point that I was going to make, into my response, but it's basically that in terms of the information that MITRE shares out, generally speaking we will chop off all of the information that's MITRE-specific. We try to share enough information that the people that we share with can build detection mechanisms on top of what we share them, so we can, you know, maybe share specific technical details about the mail clients that connected to our mail servers, who was sending them, what IP addresses they were coming from. But we typically won't share like recipient e-mail addresses, how we think they—well, we won't necessarily do the specific reconnaissance that they got against us but maybe we'll share some of their methods. So MITRE has a lot of—it's like my e-mail address is out there a lot on the STIX and TAXII discussion lists, and those are good harvesting grounds for threat actors.

ANTONIO SCURLOCK: Okay. Roger that. So, let's, let's say we have a best case scenario. The infrastructure architecture is in place, we're doing our sharing, and I'll propose two pieces of this. One, in this utopian society, everyone is tagging their data appropriately, and, I mean, for

everything—providence, utility, dissemination, and so on and so forth. And on the consumer side, they all have the capability to read, parse, execute, implement those particular tags.

I'd like you to take on two separate roles in minds for the answer. The first role is the producer. In this environment where you're tagging appropriately, and you understand that your, your consumer group can execute those tags, what, what type of feedback , as a producer, are you looking for from that consumer? What do you want to know that can help you plausibly get better indicators, better information, help you to enrich whatever you're shooting back the next time? What kind of feedback would you think you'd want?

MARK DAVIDSON: So it sounds to me like the two dimensions you mentioned are somewhat orthogonal. So there's one where it's—I guess basically as a basic sanity check, let me know if I sent you something that according to my rules I shouldn't have. That might be a first order of business. But I think that the general marking and resharing and controlling of indicator movement across organizations is kind of a separate process than getting feedback on iterating over and managing the quality of an indicator. Actually, now that I've said they're orthogonal I've talked myself into believing that they're together. I would be very interested in knowing where those controls prevented them from giving me quality feedback about an indicator. That might be a critical processing piece to know about.

ALLISON BENDER: Right. One thing I think to think about is, in terms of feedback, is, you know, how close are the relationships in the first place. If part of the trust community rules that you've establish are the sources going to be anonymized, you know, how do you track the value of an indicator? Because there was a unique ID? Is that sufficient for the group to have confidence about how their data is being shared? Are you asking for, you know, repeat citings, or changing in TTPs that reference back to an original indicator? I think the trust community really has to think about, you know, how much they're willing to share and how much feedback they want, because feedback is going to go to, most likely, being able to identify your source.

ED WHITE: And you just took my answer so I can't actually go down that path. I would—I agree on both counts. You've got a situation where the only value that this piece of information has is going to—it's only going to be beneficial to the guys as it enriches moving forward. So it may, it may come in looking at, looking like one thing, and I might give it to Allison and she might go, "Oh, my God, you know, what? This is a piece, an artifact that goes along with it." And then she gives it to Mark, and, you know, the next thing he knows he goes, "I have the attribution source, right?" And now we have a complete picture of the attacker or the attack, and, in turn, can hopefully pass that along to the community as a whole so they can be better protected.

So, you know, looking at it from a, a provider perspective, as the ISAO owner, getting that piece of information, you're going to want to see how that, that information is abridged over time, as you mentioned, but more importantly, who's touched it, right, and have that be given to you and dynamically updated so everybody else can use it, and making sure that closed loop is tracked 100 percent, right? In the end, a provider is only as good as the data that he's got,

right, and the ISAO is only as good as the community is acting as one. So the closer they are, and the more information they share, and the more willingness they have in which to be able to collectively, hopefully rise to the tide, so all boats go up, is, is going to only be beneficial in the end.

ANTONIO SCURLOCK: Outstanding. That's good, and, you know, you, you're giving me a segue into a piece of the discussion that we were having earlier, that we kind of summarized with, and I kind of started off with. One of those was with the anonymization versus the plausibility of assigning a confidence score in your data and information sharing. And I'm going to—maybe this begs the question. I don't know. But Allison, I'm going to reach to you kind of answer first. If that's the case, if that's the balance, then as a, as a consumer of information like that—and put your consumer hat on—auto-enrichment of data. It comes in, it has a confidence score of X, and you say, "Man, I've also received X from here, here, here, and here. Let me enrich that and then autosend that back out to the community with a new confidence score of X." I'm not saying that works, but I guess, give me your—if you're the consumer of information, do you auto-enrich? Do you not? Do you see pitfalls for that?

ALLISON BENDER: Sure. I mean, I think as the data consumer, any time you receive an indicator—you know, we talked about this earlier—do you know the source, and do you know what the analysis process is? You know, and at some combination, hopefully of the two, that it's going to give you a high level of confidence in the information that you're receiving. A confidence score, a reputation score, could be a part of that, kind of trying to eliminate that kind of garbage-in-garbage-out potential for automated systems, or perhaps less mature analysis from people you don't know, people you don't have a trust basis with quite yet.

So from a data consumer perspective, are you going to know the source, are you going to know the analysis, and what trust community rules are going to be established that govern whether you know the source and whether you know the analysis? To the extent that we can use reputation scores perhaps in lieu of source, that's one way to protect anonymization and the confidentiality of the data producer, but it has its own pitfalls as well, potentially that echo chamber possibility.

So I would say it really comes down to how each ISAO is going to structure its rule set on, you know, trust, consent to share, anonymization of source, and then how much data you're going to put in the information you share. Will it be a thin like indicator that can be shared quickly and easily, but high volume so that you have a lot more data points, or is what you really want, you know, that big, juicy, steak-sized indicator that has all of the wonderful analysis bits of, you know, how this previous person came to arrive at that conclusion—even if you get it late, right? So fast and light and easy, probably without the source, or, you know, really dense, really helpful, probably slow. So I think that's a balance to consider as each group thinks about what type of data they want to get and who they want to participate in that trust community with.

ED WHITE: I would agree with you, all except one point. I don't think that there's a fast versus a slow hard line. I think the technology is going to—it's there today. You can do it today. You

can get a heavy-weighted indicator, broadly speaking. To many people they're very fast. I think you've got a situation where the, the consumer of the information, automatically enriching that information and passing that information on, they have to be very diligent and make sure—back to your point—that that indicator and that process that they use is agreed upon and, and, and executed appropriately, so that it doesn't propagate itself out to, you know—the world's coming to an end and everybody goes and runs screaming down the street, right? We don't want to worry about that.

What you really are trying to get is a flexible risk score. So you want the score to be able to be managed by the individual receiving that information. So if I do have attribution from multiple sources, that I can see that I have that attribution, and because of that attribution now I have a higher risk on that individual indicator or that individual piece of intelligence, because, why? Multiple people are saying that it's bad. Then, if you do pass it on to another consumer and that person has more information, they can enrich it and they can tag it so that it can be tracked, and appropriately stated, moving forward as it relates to each individual consumer getting that information.

Now, the de-duplication piece of it, obviously you want to de-duplicate the things that are exactly the same, but the things that are going to enrich that data you obviously want to see the progression.

The other point I'd probably say that the consumer wants to make sure that they're clear on is the identification of what, what is important to them over what somebody else has deemed important for them, and, and maybe the distinction needs to be made back to the risk scoring, right? If DHS says it's bad, does that necessarily mean it's bad to your, your ISAO? Not necessarily. It could be that, just like a, a, a piece of malware on your, on your enterprise, right, that piece of malware may be attacking an OS that you don't have deployed. Is it a piece of malware? Yes. Is it bad? Yes. But is it a threat to me? No. Right? So I shouldn't have to worry about it. The same principle holds true here with the information that we're actually going to use and pass on to other people.

MARK DAVIDSON: So I think in terms of enrichment, from the MITRE info set perspective, we definitely want to enrich everything as much as possible, as soon as it comes in the door, so that within our analysis platform it's available for correlation and, you know, creation with everything else that's already in the system. So we do try and do as much of that as possible, so if you, you know, you dump an e-mail with an attachment into the system, it'll pull out the attachment, look for things in the attachment, try to carve malware out of the, like, PDF, or things like that.

Then I think to Allison's point, though, there really is, at least for us, some distinction between fast and slow, because we, you know, the, the number of malware instances in our system is closing in on like 10 million or so. So, I mean, I don't know, I know there's lots of people, or there are organizations with more than that. But we can't run deep analysis on everything single piece of malware that we bring in. So there's like this quick list of things that we can do,

and then depending on what an analyst thinks is valuable, they'll kick off processes for enriching, you know, doing that deeper dive into it. And then at the extreme degree of analysis we'll have an analyst sit down and try and reverse-engineer the piece of malware.

In terms of automated resharing, I like, I like, Ed, what you said about risk because I think, I think that's probably a—at least the way you framed it—it seems like a critical component to me, because if it's just, "Hey, I have this piece of malware," you know, that might be one thing if an adversary targeted, you know, one or two organizations with that piece of malware they'd now that at least those organizations detected that malware. But then as you add like attribution to that malware, it becomes riskier to share because now you're really showing how much you know and what your capabilities are.

But for MITRE, at least in terms of the current state of technology right now, the automated resharing is probably not a thing we'd do.

ANTONIO SCURLOCK: Roger that. So I'm going to bring you guys back and—let me pause for a minute. Are there any specific questions you want to take from the audience? Did you have any, based upon what we've covered so far?

Yes, sir. Let me get you a microphone right quick.

ATTENDEE: I was just thinking a little ways down the road as the, the information sharing operations expand, obviously there's an awful lot of defenders, there's an awful lot of attackers, there's an awful lot of activity, and it's probably never going to be any more orderly than, say, a FEMA operation, you know, during a storm. Have—you know, particularly maybe Allison from the OGC perspective, have you thought about such a thing as emergency cyber security responders, because threat information could obviously be tagged with lots of metadata so that, as it's shared in a federated network of organizations, you could try to decide what the access rights are to it. But those are also going to be contextual as well as identity-based in nature.

ALLISON BENDER: Sure. So DHS, the NCCIC, ICE, Secret Service, as well as our other partners in government—the FBI, DC3, Energy, Treasury—we all are working to try and be able to share information with each other that is important to have situational awareness of kind of the overall cyber ecosystem. But, as you point out, you know, when things tip over from, I kept blocking this over and over again, to, this is now transitioned from just an indicator to an actual incident, US-CERT, ICS-CERT, we provide a lot of different resources to the private sector. Call our 24/7 SOC, let us know what's going on. Let us know what's going on, and everything from vulnerability, scanning under our NCAT's team, to potential advice and guidance, sending in a malware sample, having a flyaway team come and provide, you know, behind the keyword "hands off" or "actual on-network assistance." All of those sorts of things are, are available, but they're very much case by case. Call us. Call who you're used to working with and say you want us to come too. We'd be happy to. I mean, we really are, in some ways, kind of like the FEMA of the Internet, right? We're, you know, the fire department as opposed to the arson

investigators. We really want to help you get back on your feet, get remediated, identify vulnerabilities in your system, and figure out ways to improve your overall security posture.

ATTENDEE: It just may be that the next level of our maturity is kind of going beyond case by case and beyond figuring out organizational processes for who shares what with whom, to who shares what based on what context, and things like that, and automating the, the different levels of response, based on the level of incident.

ALLISON BENDER: Sure. There's no requirement, there's no requirement that you call 911, and all of our services are also voluntary, so it's kind of up to each individual entity to decide, you know, yes I need some help here. And if that's the case, we're happy to.

ANTONIO SCURLOCK: I just want to jump on this from a different hat, actually, not as the moderator but from the standpoint and the viewpoint of the lead for enhanced situational awareness. You know, that context rule, information sharing piece that you talk about, and moving from there, in all honesty I believe that on the government side of the house we're kind of there, not that the machine speed and the context rule together, but definitely from the contextual to the response. In a lot of organizations, if you're prior DoD you might call that a critical information requirement. The idea that you have a preconceived concept based upon trend analysis and actually incidents that have occurred over time. You may have some sort of insight operationally into the types of things that you may want to know, without having certain specificity, and a certain threshold for that, and as that threshold is tripped you may have already preapproved or preplanned response actions and activities, whether that be a team on site, maybe some machine speed operational piece, or even what other capabilities and capacities you bring to bear, that may even be non-cyber because of, you know, laws, regulations, and authorities and whether one can actually engage or not.

So I think the contextual information sharing is not far-fetched, in the sense of going from what's currently, I would say, human and hybrid speed to machine speed. We're just not quite there yet. But I definitely think it's not just on the horizon. I think we're at a tipping point where we almost have to get there, because of what I think Ed and Mark both mentioned is the vast pieces of information that are out there. You're not going to be able to go looking for desperate data elements, but you're going to have to start looking at incidents, and actually maybe look at something a little bit more than that, not quite full-on knowledge of activity but something in there that's a little bit nebulous because you can't necessarily identify it but it's, it's strongly an indicator. And I'm not sure where that ground is.

So I think we can get there.

MARK DAVIDSON: So one area, one growing area of work that MITRE is involved in is a thing called cyber exercises, and what we try and do is help organizations basically do drills for incident response, and I'm not sure I'm allowed to say the name but there was one that we participated in probably about a month ago that was a week-long, and MITRE was in basically an observer and facilitator role, and we helped the, the people participating in the exercise—I

want to say it was a bunch of local government and others—and we helped them apply, at a high-level threat intelligence, to the processes they were doing.

So I think in terms of, you know, being able to respond to a cyber incident, I think just like any other kind of incident response, planning and exercises and drilling and, you know, basically looking at what happened after the fact and what went poorly and what went well, I think are all important pieces.

ED WHITE: I'll add one piece, from a technical point of view. We have the capability to put in place active controls that allow you to be able to, based upon, we'll call it a DEFCON 1 through 5 model, all right. As it progresses you can shut yourself completely off the Internet, right, and say, you know what? DHS has told me we're at this level, so I'm not going to let my enterprise talk to anybody until that comes back down to whatever level is acceptable to me. And you can do that today. Technology allows you to do it today. Technology allows you to do it at line speed, so that you're not propagating problems across your enterprise. And if you wanted to do that in that federated manner, in an ISAO, you could do that in the same manner, right, especially if you guys are all communicating in real time, machine to machine, right? So it comes down to both policy as well as technology, but, you know, there is the capability being able to provide you that protection, even if you want it from a, you know, a technical point of view.

ANTONIO SCURLOCK: Roger that. I'll take an opportunity to take another question or two. Let me get you a mic.

ATTENDEE: I have a question probably targeted at Mark. So automated threat indicator sharing just screams a great attack factor to me. Poisoning that information that gets shared across companies, that people rely on could have pretty horrible effects. What kind of safeguards are in place in TAXII and STIX to prevent something like that from happening?

ANTONIO SCURLOCK: Oh, is that a plant, because I have a question.

ATTENDEE: I can wait.

ANTONIO SCURLOCK: No. Go ahead.

MARK DAVIDSON: So, you know, at least in my eyes, you're completely right, you know. A big, big repository of threat indicators would be a really great thing for an adversary to get themselves on, or to, you know, hack into. In terms of STIX and TAXII, there's, there's not—so, so they're both standards. So there isn't as much necessarily built into them from a security standpoint. It's more about the application building on top of them, and implementing those standards from a security standpoint. And also in terms of we have some reference implementations for STIX and TAXII and things like that, and, you know, we've had vulnerability reports for them. We've disclosed them, we've fixed them.

And then, you know, at least to, to the extent of STIX and TAXII themselves, there haven't yet been any identified protocol or representation weaknesses that we've found, or that have been reported to us. So if you're a, if you're a vulnerability researcher and you find one, please let us know, because we, we want to fix it and we want to make it better. So maybe I can sidestep it by saying I don't know of any weaknesses in STIX and TAXII.

Was that a suitable answer?

ANTONIO SCURLOCK: That's hardcore.

ATTENDEE: [Speaking off mic.]

MARK DAVIDSON: That's going to be more, I think—it sounds to me like it's more on the back-end research part, right? We can't accept 100 percent that if I hand an IOC into the community at large that that IOC hasn't gone through some sort of QA process, for a lack of a better way to, you know, explain the situation. I would hope that there would be that process in line before we start to put it in, you know, in the machines that are blocking or in the machines that are saying I'm going to propagate it to all of the communities of interest for protection purposes, and then, to your point, there's a gigantic gaping hole across the nation's infrastructure, based upon one, one person's threat.

So I don't have the answer on how that can be done, but I, I would have to say that that has to be part of, of anything that we put forward as it relates to STIX and TAXII, IOC development, or anything.

ALLISON BENDER: A couple of things that, you know, information sharing analysis organizations might want to think about. One, very strong authentication requirements, if you're doing it in an automated fashion, right? Know who's connecting to your system if you're going to do it at machine speed and scale. Two, you know, if it's not people who are directly pumping noise into the system, are you using a time-to-live field, so that these things eventually go away, or are you testing them in some sort of controlled environment to see like, oh, wow, we're just echoing this noise but it's not real. I think it would be much harder, you know, to control adversary behavior—you know, if they decide to make a lot of noise in a lot of different places, I mean, the best, best chance we have for that is actually doing very broad, very fast indicator sharing, so that people can take appropriate action to tamp down at least that particular type of activity. But certainly if there are other ideas that you will have, that type of information would be really helpful to us.

ANTONIO SCURLOCK: I'm going to get to the last question from the audience and then we have a final topic to wrap it up for the panel—unless they told me be on unlimited time. Roger.

ATTENDEE: So it strikes me that a lot of the discussions that we're having about information sharing are things that the government in particular has solved in other contexts. If you strip away cyber there is information sharing in the intelligence community, and then law

enforcement, and there's automated or what you say computer-assisted information sharing of that kind of information. One example is the declassification problem. It's something I hear discussed among cyber threat analysts is how they wrestle through the, the risk calculation of when it's more beneficial to share among an open group, where the information might leak out and benefit the adversary, as opposed to holding in a much more close-knit group, where the adversary doesn't learn about the information. This strikes me as a problem that's been discussed for, you know, generations in other contexts.

So I'm wondering if the government has access to lessons learned from information sharing in other contexts, and best practice that could be shared in the cyber—to those of us working in the cyber context.

ANTONIO SCURLOCK: So just to be fair, I'll take a small piece of this. In a nutshell, I do believe that we do, meaning "we" the government. The key element is, is that when you talk to best practices, no matter how much you give, implementation is key, right? And we have no insight into the implemented best practices until we find out that somebody didn't implement the best practices. But I think having access to them isn't really a problem, that I'm aware of.

ATTENDEE: [Speaking off mic.]

ANTONIO SCURLOCK: So from an intelligence community or law enforcement, I can't speak to that, but I can definitely say that I know that CERT, both ICS and US, have that type of information available for the asking, and ICS-CERT even has an onsite program they would be more than happy to stop by at your request and engage with you to help you secure it.

ALLISON BENDER: So looking at the, the declassification issue, I mean, part of it is that the government has, in some ways, already structured its data, right—top secret, grave, national security risk. You go down the tier and there's these seven reasons why you can classify things, if the data is in some ways already structured. And then how do you declassify it? Typically there's an associated classification guide—this plus that is this level. You know, we don't have that level of structure that has been applied to cyber security information, because it also contains things like, you know, personally identifiable information. Is it you, the first party? Is it third-party PII, where you're getting ready to share your customer data? You know, is it proprietary information? Is it information you've received from another source?

And so, you know, certainly as we've looked at the, the declassification issues and how we can push more timely, relevant, and actionable information, and particularly that has been derived and brought down classified sources, that's been helpful, but we've had the structure to do that. We don't really have those structures available in cyber, and it takes you knowing you data and your risk levels to be able to get there.

MARK DAVIDSON: So I agree that those would be good things to learn from. I think also worthwhile to keep in mind is seemingly a key differentiator between what, you know, the law enforcement and intelligence communities might have done versus what we're doing, is, you

know, for hours today we were using Steve's Pizza Shop, or Bob's Pizza Shop, whatever it was. Joe's. And at that point the mindset becomes, how do we have the technology to prevent end users from doing something that they don't want to do? And I guess really it's a, it's a scope. There's a big scope difference, where, in terms of the intelligence community you have, you know, you have a boundary that doesn't include pizza shops somewhere.

So I think, in terms of the lessons learned, the scope of what's being tried, attempted to accomplish here, is—I'll go ahead and use the word "unprecedented," but hopefully we can find those, those lessons learned and apply them here.

ANTONIO SCURLOCK: Okay. Well, so I appreciate everybody's participation. If you don't mind, just a quick hand for the panelists that were up here, providing important feedback.

[Applause.]

ANTONIO SCURLOCK: That being said, I will at least tell you the last question I was going to ask and we'll carry it over to the next engagement, and that is, as we look at decision trees for machine-speed information, what does it mean to have the human in the loop, whether that human is doing analysis, a deeper dive on analysis, XII review, meaning any kind of II—PCII, you name it, health care data. What does that look like and what does that mean going forward in the machine-speed environment?

So I'll make sure that we catalog that question and bring it up at the next engagement for the ISAOs. And thank you of your time, and enjoy your break. Appreciate it, guys.

[Break.]

Read-Out and Next Steps in Auditorium

MIKE ECHOLS: All right. So what we want to do now is we want to have a read-out, and it's crude because we did it very quickly, but we want to give you a read-out of today. Carnegie Mellon works with us. They are going to create a white paper. What's going to happen from that white paper is it's going to inform our next session, which is going to be in Silicon Valley, the last week—don't quote me—July the 30th at San Jose State University.

ATTENDEE: Do have a hotel yet?

MIKE ECHOLS: That's what I'm telling you now. San Jose State University. The goal here is I don't want anyone's work or anyone to feel as though their work is getting tossed to the side. This is really important. It's clear to us from the conversations today, there is a lot of work to be done, and I have to tell you that I don't know of any other forum—and I haven't seen it anywhere—where all of these conversations haven't been had collectively in one place, and so the goal is to document that, right, so we know exactly where the middle of this target is, all right?

So when we go into this next meeting, we're going to be able to take the information from the day and have a more targeted approach. When the standards organization is stood up, they shouldn't have to have exactly the same conversations. We don't need to waste any time. We need to understand those things that are possible and those things that are really more long term, and so by your activities here today, that helps us to get there.

So, without further ado, I'm going to bring up Roman, and he's going to give you a read-out. And additionally, please, please, please, please, please, the good, the bad, and the ugly. Contact me. Let me know. If you think it stunk today, I want to know. That's informative to me. That's not like junk mail to me. I need to know, right? If it was wonderful, if there's another approach, whatever it is, contact me. It does not way that we are going to take your input and run with it, but potentially some of your input will be used going forward. Please contact me. Thank you.

ROMAN DANYLIW: Good afternoon, everyone, and I fully appreciate it's the end of the day. So what I have here today is just a very, very quick summary of what happened across the tracks. The way I would characterize it, it's probably more informative if you were in the track which you are about to see because they're very macro-level—macro-level topic areas.

So Track 1 largely focused on what the models might be for information sharing, the lessons learned, and the foundational things that would be important to standing up an ISAO. Some of the key themes that came through were, first and foremost, ISAO should serve their members. There's a capacity-building dimension to this ISAO, and for all ISAOs to be successful, there needs to be more workforce capacity.

There will be baseline standards published by the SO. However that is done, it needs to really take in account the diversity of capability, capacity, and the missions that the various ISAO organizations may have. ISAOs are going to serve many different types of memberships, small, medium, large, and that again needs to be captured in what makes for a successful ISAO.

With a name, include "sharing" and "analysis," but they shouldn't be considered one word. They are both as a sharing function and an analysis function, and both must be equally considered. And it's also important to recognize when one talks about sharing that there are a lot of other initiatives, a lot of other efforts, and a lot of lessons learned about how that's done and that's done today. And that needs to be folded into the ISAO process.

Areas of discussion that we went through were, first and foremost, the degree to which the government involvement would exist in recognizing ISAOs, talking through what's the value proposition of even participating in an ISAO, what the economics of that would be, the benefits that the U.S. government should give organizations that are recognized as ISAOs.

There was a little bit of a chicken-and-egg discussion about how do we talk about governance before we talk about the things that the ISAO should be doing, and we need to recognize that.

And one of the succinct bits of feedback that came up a couple of times is that there was a feeling that the standards organization, the SO, as we talk about, and all the different things that it's supposed to be doing may be misnamed as a standards organization. And that might be a source of confusion.

Pivoting to Track 2, the analysis track, that was focused on what would be some of those analytical capabilities that an ISAO would have. Some of the key themes that came from that is that the SO in its exploration of those baseline guidelines and standards should absolutely reuse existing models, taxonomies, things already out there in the community. There would be great value in having common terminology for different ISAOs to use and members, so everyone would very much understand themselves.

There was also talk about that the SO shouldn't say anything that might constrain the abilities to provide its necessary services. So again, ISAOs really need to deliver on what its members want, and there was a recognition that any kind of certification process would be challenging because of the diversity of different types of ISAOs that may be spun up, so more discussion is needed.

When thinking about data protection, given the kinds of things that an ISAO would be aggregating, there is real concern to use a lot of the existing industry standards there and reinvent only when required, and member organizations already are governed by any number of contractual regulatory requirements. And anything that the ISAO might say shouldn't conflict with that.

The data that's being shared by members or ISAOs with other ISAOs, there's a need to have originator control; that is, the ability of the organization that is sharing that information to be able to specify how that's ultimately being used. And then, of course, to do a lot of this analysis, there needs to be capacity to do so, so there's a need for training and education to have the right workforce and to know how to implement a number of these analytical activities.

Pivoting to Track 3 that was focused on automated indicator sharing—and there was a number of kind of topics explored here about what might be required to do that, what would be the responsibilities in that sharing, how to best control and handle that information, and what might be some of those technical requirements that the ISAOs should have. A couple of key takeaways were that, again, organizations that are members of ISAOs—and even the ISAOs themselves would vary in size and flavor, and there needs to be an understanding of how that market segmentation may come out and understanding how that might ultimately impact, impact indicator sharing, whether it's something as simple as volume.

There is a real need for a common language to make it easier to share, and the common language was really focused on kind of tagging of that data or perhaps formats, but there is also a recognition that interoperability really is the key, so raw formats with some context actually might be acceptable, and the recognition, very practically, it's nice to talk about those formats,

but it's likely that ISAOs are going to have to accept lots of different information, regardless of whether it's in some blessed set of formats.

To preposition effective communication, it might be—it might be good to have predefined relationships that would allow success to occur so—and there would be trust there when information arrives from different organizations.

When speaking about what might be shared, it's clear that it must be actionable, and of course, as talked about independently in other tracks, there were previously done things in information sharing, what are the lessons learned, what can be done there to tee up what the SO ultimately does.

There's almost a community, a community of norms that should come out of this about how ISAOs and members will share information, and there was discussion on what would be those obligations written, and written about how that information should occur, and a thread about, ultimately, what would be the cost of breaking some of those social norms, and what would be the governance associated with that.

And with that, that's the summary of what we had that's occurred all across the tracks. That is, by no means, comprehensive. That, by no means, covered everything that was talked about. It was a great series of conversations in Track 1, and I hear it's great in Track 2 or 3. Please look out for the white paper that should be published in a couple weeks. There will be significantly much more—significantly more comprehensive about everything that was discussed in all the tracks, and again, this will be the basis for what will be discussed in the future meeting in San Jose.

Yes, Larry.

ATTENDEE: Are the slides from today going to be made available generally?

ROMAN DANYLIW: Sir, can the slides be made available?

[No audible response.]

ROMAN DANYLIW: Yes, the slides can be made available through the website.

ATTENDEE: [Speaking off mic.]

ROMAN DANYLIW: Through the engagement website or through the mailing list perhaps? It will be sent out through the mailing list.

ATTENDEE: Thank you.

ROMAN DANYLIW: Other questions?

ATTENDEE: [Speaking off mic.]

[Laughter.]

ROMAN DANYLIW: Yes, sir.

ATTENDEE: Will the white paper be delivered to attendees, like e-mail or something?

ROMAN DANYLIW: The white paper will be produced, of course, to—DHS will get it, and from there, it will be distributed through the mailing list. It will be distributed through the mailing list.

MIKE ECHOLS: So the white paper needs to inform the next meeting, so we definitely want to make sure that you get that. What we will try to do is get it out to you guys a few days before we post it.

ROMAN DANYLIW: Okay, perfect. Again, thank you for all your participation.

MIKE ECHOLS: All right. A couple of announcements. When you exit, exit straight out these doors. Do not go through the front of the building. I really appreciate you guys attending, participating. This is a slow process, but we are making progress because we are here, and we are getting it done.

So thank you. Again, reach out to us, isao@hq.dhs.gov. Thank you.

[Applause.]